NetScaler 控制台服务

Machine translated content

Disclaimer

Contents

概述

January 29, 2024

NetScaler 控制台服务（以前称为 NetScaler ADM 服务）是一种基于 Web 的解决方案，用于管理所有 NetScaler 部署，包括 NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler SDX、NetScaler CPX、NetScaler BLX 和 NetScaler Gateway 部署在本地或云端的 Gateway。

您可以使用此云解决方案从单一、统一和集中的基于云的控制台管理、监视和故障排除整个全球应用程序交付基础结构。NetScaler 控制台提供在 NetScaler 部署中快速设置、部署和管理应用交付所需的所有功能，并可对应用运行状况、性能和安全进行丰富的分析。

NetScaler 控制台具有以下优点：

- 敏捷—易于操作、更新和使用。NetScaler 控制台的服务模型可通过云端获得，因此易于操作、更新和使用 NetScaler 控制台提供的功能。更新频率与自动更新功能相结合，可快速增强 NetScaler 部署。
- 更快实现价值—更快地实现业务目标。与传统本地部署不同，您只需点击几下即可使用您的 NetScaler 控制台。您不仅可以节省安装和配置时间，还可以避免在潜在错误上浪费时间和资源。
- 多站点管理 -单一管理平台，适用于跨多站点数据中心的实例。使用 NetScaler 控制台，您可以管理和监视处于各种部署类型的 NetScaler。您可以对部署在本地和云端的 NetScaler 进行一站式管理。
- 运营效率—优化和自动化的方式，以实现更高的运营效率。使用 NetScaler 控制台可以节省维护和升级传统硬件部署的时间、金钱和资源，从而降低运营成本。
- 实时 **Internet** 流量的可见性 - 通过实时 Internet 流量分析增强用户体验。使用 NetScaler Console，您可以在客户访问云端、数据中心和 CDN 上的应用时从他们那里收集真实的用户监视数据，并全面了解互联网健康状况。流量被引导到延迟最低和可用性最高的地点，以确保最佳的用户体验。
- 多站点应用程序 -在多个站点创建、配置和交付应用程序。使用 NetScaler Console，您可以在多个云环境中配置、交付和管理应用程序，以实现高可用性和可靠性。

NetScaler 控制台的工作原理

NetScaler 控制台作为一项服务在 Citrix Cloud 上提供。注册 Citrix Cloud 并开始使用服务后，请在网络环境中安装代理或在实例中启动内置代理。然后，将要管理的实例添加到服务中。

代理支持 NetScaler 控制台与数据中心中的托管实例之间的通信。该代理从您网络中的托管实例收集数据并将其发送到 NetScaler 控制台。

当您将实例添加到 NetScaler 控制台时，它会隐式地将自己添加为陷阱目标并收集该实例的清单。

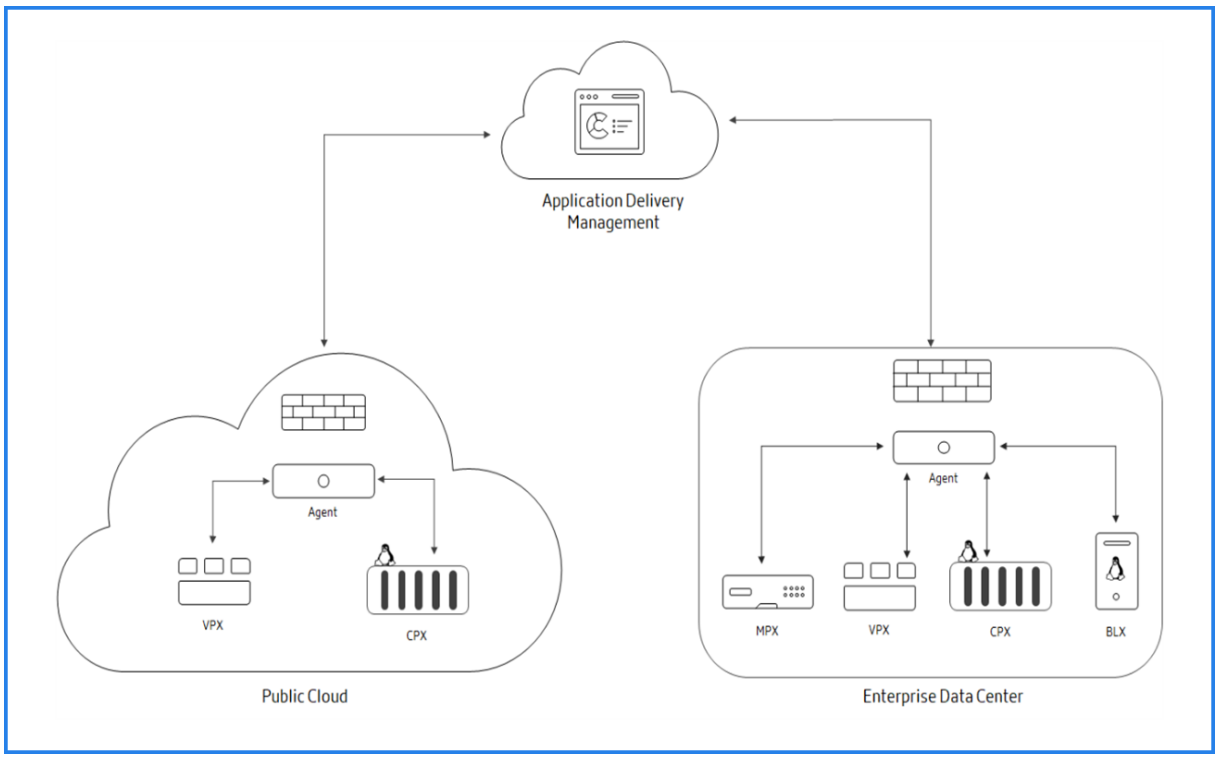
该服务收集实例详细信息，例如：

- 主机名

- 软件版本
- 正在运行和保存的配置
- Certificates（证书）
- 在实例上配置的实体等。

NetScaler 控制台定期轮询托管实例以收集信息。有关详细信息，请参阅数据治理。

下图说明了服务、代理和实例（MPX、VPX、CPX、BLX）之间的通信：



要加入 NetScaler 控制台并了解其工作原理，请参 见入门及其子主题。

功能和解决方案

January 29, 2024

本文档介绍了 NetScaler 控制台支持的功能。

应用程序分析和管理

NetScaler 控制台的应用程序分析和管理功能强化了以应用程序为中心的方法，可帮助您应对各种应用交付挑战。这种方法使您可以查看应用程序的运行状况得分，帮助您确定安全风险，并帮助您检测应用程序流量中的异常情况并采取纠正措施。

- 应用程序性能分析：App Score 是评分系统的产物，用于定义应用程序的性能。它显示应用程序在响应方面的执行情况是否良好，是否不易遭受威胁，以及所有系统是否已启动并运行。
- 应用程序安全分析：应用程序安全控制面板提供应用程序安全状态的整体视图。例如，它显示安全违规、签名违规和威胁指数等主要安全指标。应用程序安全控制板还显示发现的 NetScaler 实例的攻击相关信息，例如 SYN 攻击、小窗口攻击和 DNS 淹没攻击。
- 智能应用程序分析： 智能应用程序分析功能为监视和故障排除通过 NetScaler 设备交付的应用程序提供了一种简单且可扩展的解决方案。Intelligent App Analytics 不仅监视所有级别的应用程序交易，而且还使用机器学习技术来定义网络中的正常流量模式并检测异常。此功能减少了总体周转时间并改善了应用程序的总体正常运行时间。

样书

样书简化了为应用程序管理复杂的 NetScaler 配置的任务。样书是可以用来创建和管理 NetScaler 配置的模板。您可以创建样书来配置 NetScaler 的特定功能，也可以设计样书来为企业应用程序部署（例如 Microsoft Exchange 或 Skype for Business）创建配置。

实例管理

使您能够管理 NetScaler、NetScaler Gateway 和 Citrix Secure Web Gateway 实例。

事件管理

事件表示托管 NetScaler 实例上发生的事件或错误。例如，当系统出现故障或配置更改时，NetScaler 控制台上会生成和记录一个事件。以下是您可以使用 NetScaler 控制台配置或查看的相关功能：

- 创建事件规则
- 使用 NetScaler 控制台导出系统日志消息

证书管理

NetScaler 控制台为您简化了证书管理的各个方面。通过一个控制台可以建立自动化策略以确保合适的颁发者、密钥强度和正确的算法，同时密切跟踪未使用或即将过期的证书。

配置管理

NetScaler 控制台允许您创建配置任务，帮助您轻松地在多个实例上执行配置任务，例如创建实体、配置功能、复制配置更改、系统升级和其他维护活动。配置作业和模板将最重复的管理任务简化为 NetScaler 控制台上的单个任务。

配置审核

让您能够监视和识别您的实例中的配置的异常情况。

- 配置建议：允许您识别配置异常。
- 审核模板：允许您监视特定配置中的更改。

许可证管理

允许您通过将 NetScaler 控制台配置为许可管理器来管理 NetScaler 许可。

- NetScaler 池容量：一个通用许可证池，您的 NetScaler 实例可以从中签出一个实例许可证，并且只能根据需要多少带宽。当实例不再需要这些资源时，就会将其重新签入公用池，以使资源可用于需要它们的其他实例。
- NetScaler VPX 签入和签出许可：NetScaler 控制台根据需要分配许可 NetScaler VPX 实例。在配置 NetScaler VPX 实例时，NetScaler VPX 实例可以从 NetScaler 控制台签出许可，或者在实例被移除或销毁时将其许可返回 NetScaler 控制台。

网络报告

您可以通过在 NetScaler 控制台上监视网络报告来优化资源使用。

分析

提供一种简单且可扩展的方式来查看 NetScaler 实例数据的各种见解，以描述、预测和提高应用程序性能。您可以同时使用一项或多项分析功能。

- HDX Insight：为通过 NetScaler 的 ICA 流量提供端到端的可见性。HDX Insight 让管理员能够查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。
- Web Insight：提供对企业 Web 应用程序的可见性。它允许 IT 管理员通过提供对应用程序的集成实时监视，监视 NetScaler 提供的所有 Web 应用程序。Web Insight 使用近似算法处理来自 NetScaler 的数据。它提供了与企业中 Web 应用程序相关的指标的前 1,000 条记录。
- Gateway Insight：提供用户登录时遇到的故障的可见性，无论访问模式如何。可以查看某个给定时间登录的用户列表，以及任何给定时间的活动用户数、活动会话数及所有用户使用的字节数和许可证数。
- SecurityInsight：提供单一窗格解决方案，帮助您评估应用程序安全状态并采取纠正措施来保护您的应用程序。
- SSL Insight：提供对网络安全交易 (HTTPs) 的可见性。它允许 IT 管理员通过提供对 Web 交易的集成、实时和历史监视，监视 NetScaler 提供的所有 Web 应用程序。SSL 洞察使用近似算法处理来自 NetScaler 的数据。它提供了与企业中 Web 交易相关的指标的前 1,000 条记录。

基于角色的访问控制

基于角色的访问控制 (RBAC) 允许您根据企业内各个用户的角色授予访问权限。组织中第一个使用 Citrix Cloud 凭据登录的用户拥有超级管理员角色，默认情况下，该角色拥有所有访问权限。该组织的其他用户（后来由管理员创建）被授予非管理员角色。

订阅

提供您已购买订阅的控制面板视图。

默认情况下，您被分配到一个 Express 帐户。使用此帐户，您可以管理有限的 NetScaler 控制台资源。有关更多信息，请参见 使用 Express 帐户管理 NetScaler 控制台资源。

以下 NetScaler 控制台功能目前不可用：

- 部署
  - 从 Citrix Insight Center 迁移到 NetScaler 控制台

  - 将 NetScaler 控制台与 Citrix Virtual Desktop Director 集成
- 分析：TCP Insight 和 Video Insight
- 有限的系统设置
- 调配
  - 与 OpenStack 和 VMware NSX Manag
  - 思科 ACI 混合模式下的 NetScaler 自动化
  - 容器调配：与 Mesos/Marathon 和 Kubernetes 集成

发行说明

January 29, 2024

NetScaler 控制台（以前称为 NetScaler ADM 服务）发行说明描述了服务版本中的新功能、对现有功能的增强、已修复的问题和已知问题。

有关详细信息，请参阅：

- 新增功能
- 以前的版本

默认情况下，NetScaler 代理会自动升级到 NetScaler 控制台的最新版本。您可以在 基础结构 **>** 实例 **>** 代理页面上查看代理 详细信息。您还可以指定希望代理升级的时间。有关更多信息，请参阅 配置代理升级设置。

新增功能

September 2, 2024

2024 年 **7** 月 **25** 日

已修复的问题

基础结构　在基础结构 **>** 升级任务中，当您升级具有经典策略的 NetScaler 实例时，升级前验证会将该实例列为阻止升级的实例，并且升级不会发生。

解决办法：在升级实例之前，我们建议您将经典策略转换为 NSPEPI 工具支持的功能的高级策略。有关更多信息，请参阅使用经典策略的配置的升级注意事项。

[NSADM-113851]

遥测　作为 NetScaler 遥测程序的一部分，NetScaler 控制台不再每 24 小时检查一次以下配置，也不会将其推送到 NetScaler 实例。以前，每 24 小时检查一次配置，如果缺失，则将其推送到 NetScaler 实例：

```
enable ns feature AppFlow
add analytics profile telemetry_metrics_profile -type timeseries -
    outputMode prometheus -metrics ENABLED -serveMode Pull -schemaFile "
    ./telemetry_collect_ns_metrics_schema.json" -metricsExportFrequency
    300
```

[NSADM-114375]

2024 年 **7** 月 **15** 日

基础结构

在 **NetScaler** 控制台 **GUI** 中查看和导出 **NetScaler** 拥有的 **IP** 地址　现在，您可以在 NetScaler 控制台 GUI 中查看和导出 NetScaler 拥有的 IP 地址（基础架构 **>** 实例 **> NetScaler** 拥有的 **IP**）。

有关更多信息，请参阅查看 NetScaler 拥有的 IP 地址。

[NSADM-88798，NSADM-91769]

许可

在 **Flexed** 许可控制面板中查看在 **SDX** 实例上预置的 **VPX** 实例的详细信息　在 Flexed Licensing 控制面板（**NetScaler** 许可 **>** 灵活许可 **>** 控制板）中，在“许可的 **NetScaler**”下，您可以查看为 NetScaler SDX 签出的 VPX 实例的数量。现在，您可以单击计数来查看该 SDX 的预配置 VPX 实例详细信息，例如实例名称、IP 地址、吞吐量 (MBPS) 和版本。

之前，您只能查看为该 SDX 签出的 VPX 实例总数。

[NSADM-105358]

在零容量许可证中查看 **MPX/SDX** 主机 **ID** 和序列号的详细信息　在 **NetScaler** 许可 **>** 零容量许可中，您现在可以查看 MPX 和 SDX 实例的主机 **ID** 和序列号详细信息。

[NSADM-100327]

已修复的问题

2024 年 7 月 15 日版本中解决的问题。

基础结构

- 当您在 NetScaler 控制台（基础结构 > 实例 > NetScaler）中修改实例时，例如更改站点或管理配置文件，与该实例关联的标签的键值对会相反。

  [NSHELP-38083]

- 在配置作业中，当您在高可用性对中的主 NetScaler 和辅助 NetScaler 上同时运行 ShowConfiguration 模板时，单击下载结果文件将仅下载辅助实例的文件。

  [NSHELP-37831]

- 当网络报告（基础结构 > 网络报告）中不存在控制板时，您会收到以下错误消息：

  “您无权访问此页面”

  此错误消息可以忽略，它不会阻止您创建控制板。

  [NSADM-113332]

- 使用内置代理配置 NetScaler 控制台服务时，不会接收 SNMP 陷阱。

  [NSHELP-38191]

样书　在 NetScaler 控制台 GUI 中，当您编辑配置包以使用其他样书时，升级无法按预期进行。

[NSADM-110351]

2024 年 **7** 月 **9** 日

支持识别和修复 **CVE-2024-5491** 和 **CVE-2024-5492**

NetScaler 控制台服务安全通告现在支持识别和修复 CVE-2024-5491 和 CVE-2024-5492。

- 识别 CVE-2024-5491 需要将版本和配置扫描相结合。
- 识别 CVE-2024-5492 需要进行版本扫描。

修复需要将易受攻击的 NetScaler 实例升级到具有修复程序的推荐版本。

> 注意：
>
> 安全公告不支持已到达生命周期已结束 (EOL) 状态的 NetScaler 版本。我们建议您升级到 NetScaler 支持的内部版本或版本。

有关如何使用 NetScaler 控制台升级 NetScaler 实例的更多信息，请参阅使用作业升级 NetScaler 实例。

有关更多信息，请参阅安全公告。

> 注意：
>
> 安全公告系统扫描可能需要几个小时才能得出结论，并在安全公告模块中反思 CVE-2024-5491 和 CVE-2024-5492 的影响。要更快地查看影响，可以单击“立即扫描”开始按需扫描。

2024 年 **6** 月 **18** 日

遥测

NetScaler 遥测计划　作为 NetScaler 控制台的现有客户，您需要遵守需要收集许可和功能使用遥测数据的 NetScaler 遥测计划。遥测数据每隔 24 小时自动上载一次，您无需采取任何操作。

- 有关更多信息，请参阅 NetScaler 遥测计划。
- 有关遥测参数的更多信息，请参阅数据治理。

[NSADM-113300]

2024 年 **6** 月 **11** 日

分析

在虚拟服务器级别启用指标收集器和精益期使用情况分析　现在，指标收集器和精益使用情况分析已在虚拟服务器级别而不是实例级别启用。借助此增强功能，指标收集器和精益使用情况分析仅在流量大的活跃虚拟服务器上保持启用状态。

通过导航到“设置”**>**“分析配置”，然后单击“虚拟服务器指标摘要”下的“配置指标”，您可以查看虚拟服务器并启用指标收集器并在其他虚拟服务器上精益使用情况。

有关更多信息，请参阅配置智能应用程序分析。

[NSADM-111609]

在 **NetScaler** 实例中分配网络配置文件以收集指标　当您在 NetScaler 控制台中为虚拟服务器启用指标收集器时，来自 NetScaler 的指标数据将通过 NetScaler 子网 IP 地址 (SNIP) 导出到 NetScaler 控制台。在某些情况下，SNIP 可能会因为网络中的防火墙而被阻止。在这种情况下，您可能必须使用不同的 IP 地址。有关网络配置文件的更多信息，请参阅使用指定的源 IP 进行后端通信。

现在，您可以为 NetScaler 实例分配网络配置文件以收集指标。指标收集器将 NetScaler 计数器数据推送到 NetScaler 控制台，该控制台用于检测应用问题。导航到基础结构 **>** 实例 **> NetScaler**，选择实例，然后从“选择操作”列表中单击“为指标收集器配置网络配置文件”。

有关分配网络配置文件的更多信息，请参阅为托管 NetScaler 实例分配网络配置文件。

[NSADM-111138]

可观测性集成-查看 **NetScaler** 订阅失败的详细信息　在可观测性集成中，当您配置 NetScaler 对 Splunk 或 Prometheus 的订阅时，您现在可以查看订阅失败的详细日志。作为管理员，您可以使用这些日志分析订阅失败的原因。

有关更多信息，请参阅查看失败配置的日志

[NSADM-109022]

在可观测性集成中移除 **WAF** 和 **Bot** 洞察力的定期导出选项　现在，当您配置将见解从 NetScaler 控制台导出到可观察性工具（例如 Splunk、New Relic 和 Microsoft Sentinel）时，WAF 和机器人洞察的定期导出选项将被删除。由于 WAF 和 Bot 违规行为至关重要，因此建议使用实时导出选项在发生见解时实时导出见解。

任何具有 WAF 和 Bot 定期导出配置的现有订阅都将自动更改为实时导出。

[NSADM-109019]

基础结构

支持“基于应用程序”的配置　NetScaler 控制台服务为 AWS 和 Azure 引入了“基于应用程序”的配置。此功能简化和简化了云数据中心中的 NetScaler 部署，从而实现了从这些环境高效交付应用程序。

有关更多信息，请参阅 AWS 中基于应用程序的配置和 Azure 中基于应用程序的配置。

[NSADM-108491]

已修复的问题

2024 年 6 月 11 日版本中解决的问题。

分析

- 由于内存损坏，NetScaler 控制台/代理中的进程可能会崩溃。

  [NSHELP-38032]

- 在 **Web Insight** 中，在内容交换虚拟服务器后面配置的负载平衡虚拟服务器的详细信息在每日、每周和每月报告中不可见。

  [NSHELP-37713]

基础结构

- 当非管理员用户尝试在 NetScaler 控制台（基础结构 **>** 网络功能）中查看虚拟服务器的统计信息时，会出现以下错误消息：

  “无权访问”

[NSHELP-37977]

- 在 HA 设置中，当您使用内置代理“mastools”以及分区时，在 SSL 控制面板（基础结构 **>** **SSL** 控制面板）和负载平衡（基础结构 **>** 网络功能 **>** 负载平衡）中，辅助 NetScaler 实例的状态为“未知”。

  [NSHELP-37902]

样书

- 编辑配置包时，您对 ACL 或基于策略的路由 (PBR) 规则所做的任何更改（例如添加、更新或删除）都不会适用。

  [NSHELP-37656]

2024 年 **6** 月 **5** 日

分析

将 **NetScaler** 控制台与 **Microsoft Sentinel** 集成　在可观测性集成中，您现在可以配置 NetScaler 控制台与 Microsoft Sentinel 的集成，以便在 Microsoft Sentinel 中导出和查看见解。要成功集成，请确保满足以下必备条件：

- **Azure** 订阅 - 用于部署和使用 Microsoft Sentinel 的 Azure 订阅。
- 日志分析工作区 - 需要一个工作区来存储和分析收集的数据。
- **IAM** 角色 - 必须为工作区设置读者、贡献者等权限级别。
- 定制表 - 用于存储 NetScaler 控制台数据并将其发送到工作区。

有关更多信息，请参阅与 Microsoft Sentinel 集成

[NSADM-108930]

平台

支持 **OpenSSH** 版本 **9.x**　NetScaler 上的 OpenSSH 版本现已从 8.x 升级到 9.x。

[NSPLAT-29640]

样书

在配置包中另存为草稿选项　您现在可以将配置包另存为草稿。要将配置另存为草稿，请执行以下步骤：

1. 导航到 应用程序 **>** 配置 **>** 配置包。
2. 在“配置”页面上，单击“添加”。
3. 选择样本，然后单击“选择”。
4. 在“创建配置”页面上，单击“另存为草稿”。

保存的草稿显示在“待处理配置”下的“草稿配置”选项卡中。

有关更多信息，请参阅将配置包另存为草稿。

[NSADM-110734]

配置包中的计划选项　现在，您可以安排部署新创建的配置包。要为新配置包创建时间表，请执行以下步骤：

1. 导航到 应用程序 **>** 配置 **>** 配置包。
2. 在“配置”页面上，单击“添加”。
3. 选择样本，然后单击选择。
4. 在“创建配置”页面上的“执行”下，从“执行模式”列表中选择“稍后”。
5. 选择所需的时间和日期进行安排。

对于已部署的配置包，您可以安排何时发布更新以及何时删除配置包。编辑已部署的配置包时，计划选项可用。

有关更多信息，请参阅为配置包创建时间表。

[NSADM-110728]

已修复的问题

2024 年 6 月 5 日版本中解决的问题。

分析

- 概述控制板中的应用程序运行状况详细信息显示的详细信息与应用程序控制面板中的应用程序分数中提供的详细信息不同。

  [NSHELP-37720]

- 如果通过 NetScaler 控制台管理超过 25000 个虚拟服务器，则应用程序控制面板可能需要更多时间来加载详细信息。

  [NSADM-111705]

基础结构

- 当服务组状态发生变化时，事件规则无法生成预期的操作。

  [NSHELP-37616]

样书

- 当您将 IP 地址、整数或布尔型字段的值为空的集合数据添加到样书中的自定义数据源时，操作可能会失败。

  [NSHELP-37826]

- 当您从 NetScaler 控制台 GUI 创建配置包时，系统可能会返回一个引用内置托管 adc 数据源的参数的空列表。

  [NSHELP-37824]

- 当您尝试创建配置包或进行试运行时，如果满足以下两个条件，操作可能会失败：

  - 样书定义引用了组件部分中的另一本样书。
  - 当您为当前样书和引用的样书之间的属性指定“datum”类型的参数时。

  [NSHELP-37793]

2024 年 **5** 月 **22** 日

分析

使用 **SSL A+** 评级升级任务批量升级 **SSL** 虚拟服务器　在任务中，您现在可以查看 **SSL A+** 评级升级任务。应用程序控制板中现有的升级到 A+ SSL 评级流程使您一次只能升级一个应用程序。使用 **SSL A+** 评级升级任务，您可以进行批量升级。

NetScaler 控制台使用 NetScaler 安全前端配置文件检查应用虚拟服务器 SSL 配置，并识别未获得 A+ 评级的应用程序。**SSL A+** 评级升级任务显示非 A+ 评级的应用程序。作为管理员，您可以选择应用程序并进行批量升级以实现 SSL 合规性。

有关更多信息，请参阅可操作的任务和建议。

[NSADM-108164]

许可

灵活许可证报告中的实际使用情况详细信息　在灵活许可证报告控制面板（**NetScaler** 许可 **>** 灵活许可 **>** 报告）中，您现在可以查看实际带宽/吞吐量使用情况，从而可以查看消耗详情（峰值使用量和平均使用量）。此前，控制板仅显示分配和权利的详细信息。

此外，Flexed 许可证报告控制板中还提供了以下增强功能：

- 筛选以查看所选 NetScaler 实例的详细信息。
- 可以选择以 PDF、PNG 和 JPEG 格式导出详细信息。
- 带宽被重命名为吞吐容量。

有关更多信息，请参阅灵活许可证报告

[NSADM-97093]

样书

在样书中创建 **NetScaler** 策略表达式　样书 GUI 现在允许您通过从列表中选择项目来构建 NetScaler 策略表达式，从而帮助您更快、更准确地创建表达式。要使策略表达式编辑器可用于某个参数，请在样书的参数定义中指定 `is_policy_expression` GUI 属性。

有关更多信息，请参阅样书中的策略表达式。

[NSADM-12651]

已修复的问题

2024 年 5 月 22 日的内部版本中解决的问题。

基础结构　在配置作业中，当您在高可用性对中的主 NetScaler 和辅助 NetScaler 上同时运行 **ShowConfiguration** 模板时，单击下载结果文件将仅下载辅助实例的文件。

[NSHELP-37831]

样书　当您从 NetScaler 控制台删除使用子网 IP 地址 (SNIP) 进行管理访问的 NetScaler 实例，然后重新添加该实例时，在删除该实例之前创建的配置包上的操作可能会失败。

[NSHELP-37786]

2024 年 **4** 月 **23** 日

分析

支持导出定制 **NetScaler** 实例的定期数据　当您为 NetScaler 控制台的数据导出到 Splunk 或 New Relic 创建订阅时，您现在可以选择“定期导出”（每日或每小时）并将其应用到自定义实例。之前，不支持定期将见解数据导出到自定义实例。

[NSADM-109020]

基础结构

有关磁盘利用率的其他事件警报　NetScaler 控制台现在允许您为磁盘使用率警报设置额外的阈值。使用此阈值，您可以设置较低级别的限制，以便在突破阈值上限之前接收警报。要配置较低级别的阈值，请导航到“设置”**>**“**SNMP**”**>**“编辑”，然后启用“配置低级别阈值”。

有关更多信息，请参阅配置和查看系统警报。

[NSADM-97285]

已修复的问题

2024 年 4 月 23 日的内部版本中解决的问题。

基础结构

- 当您尝试在基础架构 **>** 实例 **> NetScaler** 中将 NetScaler 控制台报告作为快照导出时，该页面变得没有响应。

  [NSHELP-37689]

- 如果在 NetScaler 控制台中通过代理管理 10 个以上的 NetScaler 实例，则代理清单子系统会出现故障。因此，NetScaler 控制台无法获取最新的 NetScaler 配置数据。

  [NSHELP-37749]

许可

- 灵活许可证控制板上显示的实例数量不正确。

  [NSHELP-37733]

安全性

- 当您通过“安全”**>**“安全违规”**>**“所有违规”**>**“违规详情”中的“立即导出”或“计划导出”选项以表格形式导出违规记录时，无论在“要导出的记录数”中选择了多少记录，报告中都只包括当前页面视图中可见的记录。

  [NSHELP-37562]

2024 年 **4** 月 **10** 日

分析

可观测性集成**-**支持配置将 **NetScaler** 指标和审核日志导出到 **Splunk** 在设置 **>** 可观测性集成中，您现在可以配置将 NetScaler 指标和审核日志导出到 Splunk。

有关更多信息，请参阅配置将 NetScaler 指标和审核日志导出到 Splunk。

[NSADM-108858]

基础结构

通过主机名访问 **NetScaler GUI**　现在，当您通过基础架构 **>** 实例 **> NetScaler** 连接到 NetScaler 时，单击主机名即可通过主机名建立与 NetScaler GUI 的连接。以前，单击主机名或 IP 地址会启动通过 NSIP 与 NetScaler GUI 的连接。

[NSADM-108790]

查看升级期间高可用性节点之间的差异　现在，在升级 NetScaler 高可用性部署时，您可以查看主节点和辅助节点之间的配置差异。您可以查看差异并决定继续或停止升级。要使用此功能，请导航到 基础架构 **>** 升级作业，然后在“升级前 验证”选项卡中查看差异。

有关更多信息，请参阅升级任务。

[NSADM-103826]

已修复的问题

2024 年 4 月 10 日的内部版本中解决的问题。

基础结构

- 当系统日志消息包含上标等特殊字符时，基础架构 **>** 事件 **>** 系统日志消息页面显示为空白。

  [NSHELP-37551]

- 当 SSL 证书具有证书链时，基础架构 **> SSL** 控制面板 **>** 使用情况中显示的已用和未使用证书的数量不正确。

  [NSHELP-37469，NSADM-106867]

许可

- 代理进程重新启动后，代理所需的池化或灵活许可证所需的端口 27000 和 7279 可能会不可用。在这种情况下，使用池化或灵活许可的 NetScaler 实例可能会进入宽限期。

  [NSADM-110461]

安全性

- 导航到“安全”**>**“**WAF** 建议”时，可能会看到以下错误消息：

  “访问数据端点时出现 **HTTP** 错误 **500**（**[**对象对象**]**）**:** 应用程序”

  [NSHELP-37598]

2024 年 3 月 26 日

已修复的问题

2024 年 3 月 26 日的内部版本中解决的问题。

基础结构

- 创建或更新升级任务时，当您尝试在基础架构 > 升级作业 > 创建作业 > 选择实例 > 添加实例中选择实例时，添加实例页面会显示不适用于工作流程的“分区”选项卡。如果选择分区，则该页面将无响应，您无法继续操作。

  [NSADM-110118]

- 当您在“设置”>“通知”>“**Slack**”>“创建 **Slack** 通知”中创建 Slack 通知并选择“带附件的通知”时，不会显示通知，并且会看到以下错误消息：

  ```
  Invalid token
  ```

  [NSHELP-37313]

样书

- 如果在“设置”>“管理”>“系统配置”>“基本设置”中选择“仅限安全访问”选项，并且尝试执行任何设备 API 代理操作，则操作将失败。

  [NSHELP-37368]

2024 年 3 月 12 日

许可

支持在 **NetScaler** 控制台服务中手动选择 **NetScaler** 代理作为 **LSA**　现在，您可以手动选择 NetScaler 代理作为 NetScaler 池化许可或 NetScaler 灵活许可的许可服务器代理 (LSA)。

当 LSA 出现故障时，NetScaler 控制台服务会等待 24 小时才能自动选择下一个 LSA。在此期间，管理员可以使用此功能手动选择新的 LSA。但是，管理员必须确保当选的新 LSA 的状态为已启动且其诊断状态为正常。

有关更多信息，请参阅灵活或池化许可的 NetScaler 代理行为。

[NSADM-105168]

已修复的问题

2024 年 3 月 12 日的内部版本中解决的问题。

分析

- 当您为网关虚拟服务器启用 **Gateway Insight** 时，设置 **>** 分析配置 **>** 所有虚拟服务器中的分析状态列显示已禁用。

  [NSHELP-37400]

- 在网关 **> Gateway Insight** 中，身份验证选项卡不显示身份验证失败的用户详细信息。

  [NSHELP-37465]

基础结构

- 创建用户定义的策略并将用户添加到该策略时，针对特定资源的 GET API 请求会遇到权限问题并显示以下错误：

  “由于未授予所需权限，因此未获得授权”

  [NSHELP-37331]

2024 年 **2** 月 **28** 日

基础结构

VIP 许可和 **NetScaler** 控制台服务存储的更新

- **NetScaler** 控制台服务上不受限制的 **VIP**：自 NetScaler 控制台服务版本 14.1-21.x 起，许可的 VIP 概念被移除。现在，NetScaler 控制台服务中提供了无限数量的 VIP。您不再需要购买 NetScaler 控制台虚拟服务器许可证，因为 VIP 许可 SKU 将很快变为销售终止 (EOS) 和续订结束 (EOR)。
- **NetScaler** 控制台服务存储：
  - NetScaler 控制台服务存储 SKU 将很快终止销售 (EOS) 和续订结束 (EOR)。
  - 现在，默认 NetScaler 控制台服务存储权限为 5GB。
  - 过去购买的任何 NetScaler 控制台服务存储许可将在期限结束之前兑现。
  - 过去购买的任何 NetScaler 控制台 VIP 许可证，只要您有权获得相应的 NetScaler 控制台服务存储，则将在期限结束之前兑现。
  - 如果您购买了任何其他授权包，使您有权获得更高的 NetScaler 控制台存储权限，则默认 5GB 将更改为与授权相匹配。

[NSADM-108300]

分析和指标收集器的更新

- 从 14.1 21.x 版本开始，VIP 支持无限制，所有现有和新的虚拟服务器现在都将自动获得许可。您可以在虚拟服务器上启用分析，而无需明确授予其许可。

- 现在，在 NetScaler 控制台中从 14.1 21.x 版本中添加的新 NetScaler 实例中的所有 NetScaler 许可类型中，默认禁用指标收集器。现有托管实例的指标收集器配置保持不变。

[NSADM-108803]

分析

操作策略-为应用程序使用情况配置通知　在操作策略（设置 > 操作 > 操作策略）中，您现在可以为应用程序使用配置操作策略，并选择每秒请求数、吞吐量和数据量选项。这些选项使您能够配置和接收每秒平均请求数、每秒请求异常、平均吞吐量、吞吐量异常、总数据量和数据量异常的通知。有关更多信息，请参阅配置操作策略以接收应用程序事件通知。

[NSADM-104833]

可观测性集成　与 Splunk 和 New Relic 集成的配置流程现已得到增强，以提供更好的用户体验，并可在“设置”>“可观测性集成”下找到。此前，在“设置”>“生态系统集成”下提供了与 Splunk 和 New Relic 集成的配置流程。

有关更多信息，请参阅可观测性集成

[NSADM-104702]

可观测性集成-支持配置 **NetScaler** 指标导出到 **Prometheus**　在“设置”>“可观测性集成”中，您现在可以通过选择默认架构配置 NetScaler 指标导出到 Prometheus。

有关更多信息，请参阅 Prometheus 集成和可观测性集成。

[NSADM-101426]

Gateway Insight - 对导出报告的改进　在网关 **> Gateway Insight** 中，您现在可以使用每个指标（EPA、身份验证、授权失败、SSO 和应用程序启动）下所有表格中的设置图标，仅使用选定选项导出报告。以前，无论选择了什么选项，导出的报告都会显示所有信息。

[NSADM-96821]

样书

对默认样书的更新　基于 NetScaler 版本 10.5 的默认样书将在即将发布的版本中弃用。基于 NetScaler 版本 13.0，现在可以在应用程序 > 配置 > 样书 > 默认样书中提供一套新的默认样书。

[NSADM-105513]

克隆样书的选项　NetScaler 控制台现在允许管理员创建样书的副本及其依赖项。然后，管理员可以使用此捆绑包进行其他自定义，例如更新 `parameters` 和 `components`。

要使用此功能，请导航到“应用程序”**>**“配置”**>**“样书”，选择默认或自定义样书，然后单击“克隆”。

有关更多信息，请参阅克隆样书。

[NSADM-92376]

已修复的问题

2024 年 2 月 28 日的内部版本中解决的问题。

基础结构

- 从 NetScaler 控制台迁移到 NetScaler 控制台服务失败，某些 Azure Active Directory 组在 NetScaler 控制台服务中不可用。之所以出现此问题，是因为在 NetScaler 控制台中创建的 Azure Active Directory 组名中存在空格。

  [NSHELP-37006]

- 如果用户属于多个 Azure Active Directory 组，则无法访问 NetScaler 控制台。

  [NSHELP-37005]

- 在 **Web Insight** 和 安全违规中，GUI 中的计划导出工作流程得到了增强，以提供更好的用户体验。

  [NSADM-106624]

- 在 基础架构 **>** 网络报告中，表格导出报告不包括服务、服务组、虚拟服务器和接口名称等详细信息。

  [NSHELP-37224]

- 只有在从高级带宽许可池中签出至少一个 NetScaler 后，灵活许可控制面板才会显示 NetScaler 的详细信息。

  [NSADM-106497]

2024 年 **2** 月 **6** 日

分析

应用程序控制面板**-**支持从 **NetScaler** 管理分区查看应用指标详情　在 应用控制面板中，您现在可以查看从 NetScaler 管理分区创建的应用程序的指标详情。以前，您只能查看管理分区中的应用程序，而没有任何指标。

[NSADM-105343]

基础结构

Citrix Cloud 中的 **NetScaler ADM** 品牌重塑　从 14.1 16.x 版本开始，NetScaler ADM 服务更名为 NetScaler 控制台服务。接下来，应用程序交付管理现在在以下地方更名为 NetScaler 控制台：

- Citrix Cloud 主页中“我的服务”下的图块。
- **Citrix Cloud** 菜单 **>** 我的服务中的服务名称。
- 在 **Citrix Cloud** 菜单 **>** 身份和访问管理 **>** 管理员 **>** 添加管理员/组中的“设置访问权限”**>**“自定义访问权限”中的“添加管理员”工作流程中的产品名称。

在升级任务中运行默认验证脚本　NetScaler 控制台现在在升级作业工作流程中加入了默认验证脚本选项。这些默认脚本在升级任务之前和之后都运行，生成差异报告。您仍然可以选择运行自定义默认脚本。

有关更多信息，请参阅升级 NetScaler 实例。

[NSADM-100803]

自动部署 **NetScaler** 控制台站点的 **Radar** 对象　NetScaler 支持自动部署 NetScaler 控制台站点的 Radar 对象，无需在 NetScaler 实例上手动部署。

此增强功能仅在编辑 NetScaler 实例时可用，并且仅适用于站点类型数据中心（专用类型）或分支机构。

当您从“真实用户测量”列表中选择“部署到 **NetScaler**”时，系统会自动填充 **NetScaler** 实例列表，允许您选择部署 Radar 对象 (r20.png) 的特定实例。

有关更多信息，请参阅自动部署 Radar 对象。

[NSADM-104691]

已修复的问题

2024 年 2 月 6 日的内部版本中解决的问题。

分析

- **XML SQL** 攻击不会在安全控制面板（“安全”**>**“安全控制面板”）和“安全违规”控制面板（“安全”**>**“安全违规”）中报告。

  [NSHELP-37159]

许可

- 只有在从高级带宽许可池中签出至少一个 NetScaler 后，灵活许可控制面板才会显示 NetScaler 的详细信息。

  [NSADM-106497]

管理和监视

- 创建配置作业时，基础架构 **>** 配置 **>** 作业中的状态显示已完成，但详细信息 **>** 执行摘要中的状态显示已完成 0%。

  [NSHELP-37176]

- 即使 NetScaler HA 升级已完成，NetScaler HA 的两阶段升级任务状态仍显示“已计划”。主节点显示已完成（状态阶段 **1**：已完成），但辅助节点显示已计划（阶段 **2**：已计划）。

  [NSHELP-36943]

- 当在“基础架构”**>**“配置”**>**“配置审核”**>**“审核模板”**>**“添加”下创建名称中包含特殊字符的配置审核模板时，该模板将成功生成。但是，在轮询期间，无法为配置审核控制板中的模板生成差异报告。

  使用-（短划线）和“_”（下划线）以外的特殊字符时会出现此问题。

  [NSHELP-36438]

2024 年 **1** 月 **24** 日

分析

在“任务”中查看“升级建议”的详细信息　在任务中，您现在可以查看升级公告可操作的任务。根据您当前的使用情况，如果您的 NetScaler 实例在 90 天内已经或即将达到生命周期终止 (EOL) 或维护结束 (EOM)，则升级公告任务将显示这些实例的详细信息。您可以单击“采取操作”，将这些实例升级到推荐的版本。

[NSADM-104715]

基础结构

增强了只读用户的权限　拥有以下功能只读权限的用户现在可以轮询 NetScaler 实例：

- SSL 证书（基础架构 **> SSL** 控制面板 **>** 立即轮询）
- 网络功能（基础架构 **>** 网络功能 **>** 立即轮询）
- 配置审核（基础架构 **>** 配置 **>** 配置审核 **>** 立即轮询）

[NSADM-104710]

已修复的问题

2024 年 1 月 24 日的内部版本中解决的问题。

- NetScaler SDX 中的内置代理注册会显示成功消息，但是 SDX 实例不会出现在基础架构 **>** 实例控制板中。

  [NSHELP-37137，NSHELP-37128]

- 在基础架构 **>** 网络功能 **>** 负载平衡中，服务器选项卡指示服务器的数量，但不为非默认用户显示任何表条目。

  [NSHELP-36964]

2024 年 1 月 16 日

支持识别和修复 **CVE-2023-6548** 和 **CVE-2023-6549**

NetScaler 控制台服务安全公告现在支持识别和修复 CVE-2023-6548 和 CVE-2023-6549。

- 识别 CVE-2023-6548 需要进行版本扫描。
- 识别 CVE-2023-6549 需要将版本和配置扫描相结合。

修复需要将易受攻击的 NetScaler 实例升级到具有修复程序的推荐版本。

> 注意：
>
> 安全公告不支持已到达生命周期已结束 (EOL) 状态的 NetScaler 版本。我们建议您升级到 NetScaler 支持的内部版本或版本。

有关如何使用 NetScaler ADM 升级 NetScaler 实例的更多信息，请参阅使用作业升级 NetScaler 实例。

有关更多信息，请参阅安全公告。

> 注意：
>
> 安全公告系统扫描可能需要几个小时才能得出结论，并在安全公告模块中反思 CVE-2023-6548 和 CVE-2023-6549 的影响。要更快地看到影响，您可以单击“立即扫描”开始按需扫描。

[NSADM-104763]

2024 年 1 月 9 日

分析

支持与其他用户共享自定义控制板　作为管理员，您现在可以与其他用户共享自定义控制板。在“概述”**>**“自定义控制板”中，选择一个控制板并单击“共享”。键入用户名并单击“邀请”以共享控制面板。分配的用户可以在只读模式下查看控制板。

[NSADM-100879]

基础结构

在 **NetScaler** 控制台站点中配置 **ITM Radar**　ITM Radar 增强了网络监视能力。部署在数据中心、虚拟机或云提供商中的站点现在可以托管 Radar 对象 (r20.png)，从而深入了解性能指标。ITM Radar 对象主动收集有价值的最终用户应用程序统计信息，为站点提供强大的 ITM Radar 遥测功能，以实现更有效的网络监视和明智的流量管理决策。

有关更多信息，请参阅配置 ITM Radar。

[NSADM-91686]

在 **Splunk** 和 **New Relic** 中查看 **Gateway Insight** 数据　当您在“设置”**>**“生态系统集成”中创建用于将 NetScaler 控制台服务与 Splunk 和 New Relic 集成的新订阅时，您现在可以选择 **Gateway Insight** 选项。使用“**Gateway Insight**”选项配置订阅后，您可以在 Splunk 和 New Relic 中查看 Gateway Insight 数据。

如需更多信息，请参阅与 Splunk 集成和与 New Relic 集成。

[NSADM-101036]

立即将 **SSL** 数据导出到 **Splunk** 和 **New Relic**　现在，管理员通过在 Splunk 和 New Relic 中选择 SSL 证书洞察创建订阅后，**SSL** 数据将立即导出到 Splunk 和 New Relic。此前，管理员必须单击“立即轮询”（基础架构 **>** **SSL** 控制面板）才能首次导出数据。

[NSADM-101035]

在“任务”中查看“升级建议”的详细信息　在任务中，您现在可以查看升级公告可操作的任务。根据您当前的使用情况，如果您的 NetScaler 实例在 90 天内已经或即将达到生命周期终止 (EOL) 或维护结束 (EOM)，则升级公告任务将显示这些实例的详细信息。您可以单击“采取操作”，将这些实例升级到推荐的版本。

[NSADM-104715]

操作策略-为请求、带宽和响应时间配置通知　在操作策略（设置 **>** 操作 **>** 操作策略）中，当您在应用程序性能中配置操作策略时，现在可以选择请求、带宽和响应时间选项。这些选项使您能够配置和接收有关总请求、总带宽、平均响应时间和响应时间异常的通知。有关更多信息，请参阅配置操作策略以接收应用程序事件通知。

此外，您现在还可以从 **Web Insight** 中的图表趋势中为这些指标配置操作策略。作为管理员，当您发现任何异常流量模式或任何应用程序的这些指标突然出现峰值时，此增强功能允许您在将相对操作策略置于图表中的特定点后单击“创建操作策略”来创建相对操作策略。

[NSADM-101273]

已修复的问题

2024 年 1 月 9 日的内部版本中解决的问题。

许可

- 应用灵活或池化许可证后，“分析配置”页面（“设置”**>**“分析配置”）不会更新正确的详细信息。

  [NSADM-106665]

- **NetScaler** 许可 **>** 灵活许可 **>** 控制板中的灵活许可控制面板显示为空白。

  [NSADM-106561]

- 在 **NetScaler** 许可 **>** 许可管理中，通过电子邮件通知对违反阈值的配置无法按预期运行。

  [NSHELP-36895]

2023 年 **12** 月 **13** 日

基础结构

NetScaler ADM 服务品牌重塑　NetScaler 应用程序交付管理服务（ADM 服务）现已更名为 NetScaler 控制台服务。

其他已更名的术语如下：

- ADM 代理现已更名为 NetScaler 代理
- ADM Service Connect 现已更名为控制台公告连接

> 注意：
>
> 我们的 NetScaler 控制台服务产品用户界面和文档目前正在更新中，以反映这些变化。在这段时间内，您可能会遇到以前的名称和更名后的名称互换引用。感谢您在过渡期间的理解。

[NSADM-105125]

许可

NetScaler 灵活许可　NetScaler 灵活许可是新的许可框架，旨在简化许可管理流程。您的灵活许可证包括软件实例许可证（VPX/CPX/BLX、SDX、MPX 和 VPX FIPS）和带宽容量许可证。您必须在 NetScaler 控制台服务或 NetScaler ADM 本地上申请灵活许可。您还必须分别在 NetScaler MPX 硬件和 NetScaler SDX 硬件上申请 MPX Z-Cap 和 SDX Z-Cap 许可。然后，您可以将它们分配给部署在云端或本地的所有 NetScaler 外形规格。

> 注意：
>
> 确保您的 NetScaler 代理运行的是 16.x 或更高版本。

有关更多信息，请参阅灵活许可证。

[NSADM-98483]

分析

灵活许可**-**在 **NetScaler** 控制台中添加的新 **NetScaler** 实例默认禁用指标收集器　如果您使用的是灵活许可，则在 NetScaler 控制台中添加的新 NetScaler 实例现在默认禁用指标收集器。必须手动启用此选项才能将 NetScaler 指标和计数器数据推送到控制台。现有托管实例的指标收集器配置保持不变。

> 注意：
>
> 必须启用指标收集器，数据才能显示在应用程序控制板及其相关选项卡中，例如该实例上所有许可虚拟服务器的性能、SSL 和关键指标。

有关更多信息，请参阅配置智能应用程序分析。

[NSADM-106193]

弃用视频和 **TCP** 洞察功能　在最新版本中，**Video Insight** 和 **TCP Insight** 报告数据不再可在 NetScaler 控制台中进行可视化。

[NSADM-106597]

基础结构

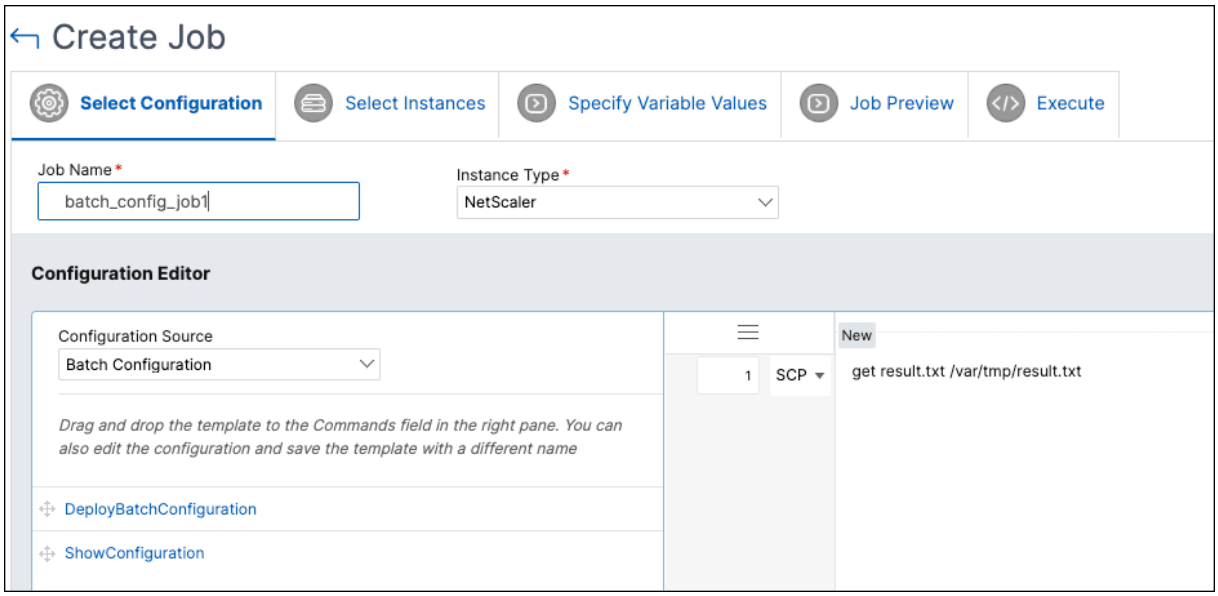
下载批处理配置任务的文件　配置作业现在允许您使用 NetScaler ADM GUI 将文件从 NetScaler 实例上的目录下载到本地计算机上的某个目录中。

要使用此功能，请导航到 基础架构 **>** 配置 **>** 配置作业，选择一个作业，然后单击 下载结果文件。

仅当满足以下条件时，“下载结果文件”按钮才可用：

- 创建的配置作业是批处理配置作业。要创建批处理配置作业，请转到 创建作业 **>** 选择配置，然后在 配置编辑器 中选择 配置源 **>** 批量配置
- 在 `scp get`配置编辑器 中使用 命令

对于多个 NetScaler 实例，下载的结果文件可在单独的文件夹中找到，每个文件夹对应一个单独的实例。



[NSADM-105442]

暂停并恢复预定的升级作业　NetScaler ADM 现在提供了暂停计划升级任务的选项。要使用此功能，请导航到 基础架构 **>** 升级作业，选择现有的计划升级作业，然后单击“停 止”以暂停作业。要恢复预定的升级作业，请单击“继续”。

> 注意：
>
> 如果在决定恢复升级任务后已过了计划时间，则需要重新创建升级作业。

有关更多信息，请参阅 升级任务

[NSADM-100807，NSADM-97280]

已修复的问题

2023 年 12 月 13 日的内部版本中解决的问题。

分析

- 在 应用程序 **>** 控制板中，将事务日志数据导出为表格或 CSV 格式不会显示任何数据。当 NetScaler ADM 配置为非 UTC 时区时，会注意到此问题。

  [NSHELP-36817]

- 在“安全”**>**“安全违规”**>**“违规详情”中，搜索过滤器无法识别“Client-IP！=”查询。

  [NSHELP-36675]

- 从“安全”>“安全违规”**>**“导出报告”**>**“计划导出”中导出 且文件格式选择为 JPEG 的预设快照报告显示以下错误：

  “请在报告上下文或 csv_export_arr 中提供查询参数。”

  [NSHELP-36657]

基础结构

- 某些用户会在 基础架构 **>** 实例 页面的地图上看到“仅用于开发目的”水印。

  [NSHELP-36863]

管理和监视

- NetScaler ADM 代理生成 “netScalerLoginFailure” SNMP 陷阱。出现此问题的原因是，由于换行符，ADM 代理用于登录 NetScaler 的凭据被截断。

  [NSHELP-36804]

安全性

- 在“统一安全”控制面板（“安全”**>**“安全控制面板”**>**“管理应用程序”）中配置保护后，不会在内容交换虚拟服务器中部署保护。

  [NSADM-105544]

2023 年 **11** 月 **29** 日

基础结构

使用标签为用户组授权实例　作为管理员，您现在可以根据关联标签向用户授权特定实例。创建用户组时，导航到 设置 **>** 用户和角色 **>** 添加 **>** 授权设置 **>** 选择标签，然后通过标签授权用户访问实例。

有关更多信息，请参阅 配置基于角色的访问控制。

[NSADM-104798]

已修复的问题

2023 年 11 月 29 日的内部版本中解决的问题。

- 当您在基础结构 **>** 实例 **> NetScaler > SDX >** 选择操作 **>** 预配 **VPX** 中在 SDX 上预置 VPX 实例时，不会出现“通过网络管理”选项。

  [NSHELP-36328]

2023 年 **11** 月 **9** 日

分析

配置网关会话超时　在设置 **>** 分析设置 **>** 配置 **ICA/**网关会话超时中，您现在可以为 Gateway Insight 配置超时会话。默认情况下，该值为 30 分钟。使用此配置，如果 NetScaler ADM 在配置的时间段内未收到会话终止记录，则会话将被记录为已终止。

[NSADM-101271]

NetScaler 备份过程和防火墙访问中的更新　NetScaler 实例备份现在直接从 NetScaler 代理上载到 NetScaler ADM 服务，然后再上载到 Amazon S3。因此，您不再需要允许访问防火墙中的 S3 URL 以获取 NetScaler 备份服务。

[NSADM-98267]

支持 **Intelligent Traffic Management** NetScaler ADM 服务现在支持 Intelligent Traffic Management，可通过实时分析 Internet 流量并自动将流量引导到最佳位置来帮助您增强用户体验。

通过 Intelligent Traffic Management，您可以：

- 根据实时服务数据，在多个地点交付应用程序，以缩短应用程序响应时间并最大限度地提高应用程序可用性。
- 配置权威 DNS 来管理您的区域。
- 查看对客户数据中心或交付平台和应用程序的见解。
- 确定最佳平台和地点。

点击左侧导航窗格中的 **Intelligent Traffic Management** 开始操作。有关更多信息，请参阅 Intelligent Traffic Management。

[NSADM-91677]

“统一安全”控制板 在 NetScaler ADM 中，您现在可以使用单窗格控制面板来配置保护、启用分析并将其部署到您的应用程序上。导航到“安全”**>**“安全控制面板”，然后单击“管理应用程序”以执行 以下操作：

- 查看所有安全和不安全的应用程序。
- 选择不安全的应用程序，使用各种模板选项配置保护，启用保护分析，然后将其部署到应用程序上以保护应用程序。

以前，您必须在 NetScaler 实例中配置所有保护，并且只能查看 NetScaler ADM 中配置的保护的分析。作为管理员，此单窗格控制板使您能够在单个工作流程中为应用程序配置保护。

有关更多信息，请参阅“统一安全”控制面板。

[NSADM-92678]

已修复的问题

2023 年 11 月 9 日的内部版本中解决的问题。

基础结构

- 在设置 NetScaler 内置代理来管理实例时，即使注册成功，配置也会停留在“添加实例”页面，并且可以在实例控制板页面中查看代理。

  [NSHELP-36614]

样书

- 当更新或删除参数中包含特殊字符的配置包时，尽管对 NetScaler 的更新或删除操作未完成，NetScaler ADM 仍会显示成功消息。通过此修复，NetScaler ADM 现在可以准确显示由于配置包定义中的特殊字符而导致的任何不完整配置的错误。

  [NSADM-104423]

2023 年 **10** 月 **25** 日

分析

创建自定义控制板以查看实例密钥指标详情　与统一控制板（概述 **>** 控制板）类似，您现在可以通过创建自定义控制板根据自己的选择查看实例指标详细信息。例如，如果您想监视应用程序和应用程序安全的关键指标，则可以通过仅选择这两个类别来创建自定义控制板。通过为每个控制板使用唯一的名称，您最多可以创建 20 个控制板。作为管理员，此增强功能使您能够创建多个控制板并仅监视所需的实例见解。

要开始使用，请导航到 概述 **>** 自定义控制板。

有关更多信息，请参阅 创建自定义控制板以查看实例关键指标详情。

[NSADM-91875]

可操作的任务和建议　任务 功能现已添加以下增强功能：

- 引入了新的 任务 选项卡，您可以在其中查看需要立即关注的可操作任务。这些任务是根据您当前的使用率显示的。作为管理员，完成这些可操作的任务可确保您的 NetScaler 部署安全、合规且高效。您还可以根据问题的严重性（严重和中等）查看这些可操作的任务。
- 待办事项选项卡已重命名为“建议”。在“建议”中，您可以继续查看现有任务，然后单击“引导我”以完成任务。
- “存档”选项卡不再可用。相反，您可以选择消除列表中的建议。

有关更多信息，请参阅可操作的任务和建议。

基础结构

使用证书存储更新 **SSL** 证书　当您在 基础架构 **> SSL** 控制面板 **>** 更新中更新 **SSL** 证书时，您现在可以从证书存储中选择证书。之前，您必须上载证书文件和密钥文件才能更新 SSL 证书。

[NSADM-101303]

更新的 **SNMP** 陷阱列表　SNMP 陷阱列表现已更新，增加了新的陷阱以及一些之前丢失的陷阱。要查看完整列表，请导航到 基础架构 **>** 事件 **>** 事件设置 **> NetScaler**。

[NSADM-99798]

已修复的问题

2023 年 10 月 25 日的内部版本中解决的问题。

- 当您在基础结构 **>** 实例 **> NetScaler > SDX >** 选择操作 **>** 预配 **VPX** 中在 SDX 上预置 VPX 实例时，不会出现“通过网络管理”选项。

  [NSHELP-36328]

2023 年 **10** 月 **10** 日

管理和监视

支持识别和修复 **CVE-2023-4966** 和 **CVE-2023-4967** NetScaler 控制台安全公告现在支持识别和修复 CVE-2023-4966 和 CVE-2023-4967。

- 识别需要同时进行版本和配置扫描。
- 修复需要将易受攻击的 NetScaler 实例升级到具有修复程序的推荐版本。

> 注意：
>
> 安全公告不支持已到达生命周期已结束 (EOL) 状态的 NetScaler 版本。我们建议您升级到 NetScaler 支持的内部版本或版本。

有关如何使用 NetScaler ADM 升级 NetScaler 实例的更多信息，请参阅使用作业升级 NetScaler 实例。

有关更多信息，请参阅安全公告。

[NSADM-101092]

2023 年 **9** 月 **26** 日

分析

仅将数据从选定实例导出到 **Splunk** 和 **New Relic** 当您创建将数据导出到 Splunk 和 New Relic 的订阅时，您现在可以选择 NetScaler 实例。如果您使用特定实例创建订阅，则仅将数据从选定的 NetScaler 实例导出到 Splunk 和 New Relic。

有关更多信息，请参阅与 Splunk 集成和与 New Relic 集成。

[NSADM-94371]

基础结构

使用 **Cloud Connector** 与 **ADM** 服务连接的 **ADM** 本地实例　在“设置”中，您现在可以查看名为 **ADM On-Prem** 的新选项。在此页面中，您可以查看通过 ADM On-Prem Cloud Connector 与 ADM 服务租户连接的 ADM 本地实例的详细信息。

有关更多信息，请参阅使用 Cloud Connector 与 ADM 服务连接的 ADM 本地实例。

[NSADM-94576]

已修复的问题

2023 年 9 月 26 日的内部版本中解决的问题。

分析

- 定期修剪应用程序控制板数据并未按预期运行。因此，NetScaler 控制台消耗了更多的磁盘空间。

  [NSHELP-36184]

2023 年 **9** 月 **13** 日

基础结构

用于上载技术支持包的身份验证令牌　现在，您需要一个身份验证令牌才能将 NetScaler 上生成的技术支持包上载到 Citrix 技术支持服务器。之前，您使用 Citrix 用户名和密码上载了技术支持包。有关更多信息，请参阅 如何为 NetScaler 实例生成技术支持包。

[NSADM-93351]

已修复的问题

2023 年 9 月 13 日的内部版本中解决的问题。

分析

- 当 NetScaler 控制台丢失虚拟服务器许可证时，预计将禁用使用这些许可证的虚拟服务器的分析状态。对于 VPN 虚拟服务器，这种情况不如预期的那样起作用。

  [NSHELP-36183]

基础结构

- 在 **Gateway > HDX Insight** 和网关 **> Gateway Insight** 中，图表的 X 轴显示日期而不是时间。

  [NSHELP-36043]

管理和监视

- 从“基础结构”**>**“网络报告”**>**“导出”中导出的报告显示为截断或不完整。

  [NSHELP-36252]

- 即使 AD 组映射到 ADM 组，属于许多 Azure 组的 Azure Active Directory (AD) 用户也无法访问 NetScaler 控制台。

  [NSHELP-35456]

August 31, 2023

基础结构

在 **SSL** 控制板下查看“证书存储”页面　现在，您可以导航到“基础结构”**>**“**SSL** 控制板”**>**“证书存储”以查看“证书存储”页面。

[NSADM-97858]

支持代理的 **SNMP** 功能　在基础结构 **>** 代理 **>** 操作 **>** 管理 **SNMP** 中，您现在可以为代理创建 SNMP 管理器、SNMP 用户和 SNMP 视图。

有关 SNMP 管理员和用户的更多信息，请参阅为 NetScaler ADM 代理创建 SNMP 管理员和用户。

[NSADM-94923]

数据存储管理控制板的用户体验和功能改进　为了改善用户体验并提高数据存储管理的效率，数据存储管理控制板现在提供了以下改进：

- 控制板的新用户界面设计：
  - 添加了数据提取、存储消耗、数据修剪和操作图块
  - 操作图块提供了添加更多存储空间、查看数据保留策略、执行数据修剪和查看系统通知的选项
- “存储消耗趋势”部分的搜索功能：

  除了查看存储趋势外，您现在还可以搜索特定的功能和趋势。

- 执行数据修剪：

- 现在，您可以选择一项或多项功能并对其数据进行修剪以释放存储空间
- 您每月有权进行 10 次数据修剪

有关数据存储管理控制板的更多信息，请参阅数据存储管理。

[NSADM-93202]

安全性

API 网关已重命名为 **API** 安全性　**API** 网关现已重命名为 **API** 安全性。您可以在以下页面中查看更改：

- 安全性 **>** **API** 安全性
- 安全性 **>** **API** 安全性 **>** **API** 分析 **>** 获取帮助 **>** **API** 安全性文档
- 设置 **>** 用户和角色 **>** 组 **>** 授权设置 **>** **API** 安全性
- 设置 **>** 用户和角色 **>** 访问策略 **>** 权限 **>** 安全性 **>** **API** 安全性

[NSADM-102384]

已修复的问题

2023 年 8 月 31 日的内部版本中解决的问题。

管理和监视

- 在“基础结构”**>**“网络报告”中，“网络报告”控制板不在虚拟服务器报告中显示任何历史数据。当您在创建控制板时在选择实体中选择 一个 NetScaler HA 对时，就会出现此问题。

[NSHELP-36228]

2023 年 **8** 月 **11** 日

管理和监视

安全公告**-**文件完整性监视　NetScaler 控制台安全公告现在使您能够扫描 NetScaler 编译文件并查看对原始 NetScaler 编译文件进行任何更改或添加的结果。

在安全公告（基础结构 **>** 实例公告 **>** 安全公告）中，“立即扫描”选项允许您选择“扫描 **CVE**”、“扫描文件”或“同时扫描”。选择“扫描文件”或“同时扫描”后，NetScaler 控制台会将托管 NetScaler 编译文件的二进制哈希值与原始二进制哈希值进行比较，并在“文件完整性监视”选项卡下突出显示是否有任何文件更改或文件添加。

扫描结果显示了 NetScaler 实例，这些实例可能对原始文件进行任何更改和/或添加任何其他文件。要对扫描结果进行进一步调查，您可以联系贵组织的数字取证。

有关更多信息，请参阅安全公告。

[NSADM-91856]

2023 年 8 月 9 日

基础结构

查看 **NetScaler VPX** 的虚拟化平台详细信息　在 基础结构 **>** 实例 **> NetScaler > VPX** 中，您现在可以通过选择“设置”**>**“云平台”来查看 NetScaler VPX 托管的平台。

[NSADM-97319]

重试失败的升级作业　在 基础结构 **>** 升级任务中，您现在可以选择失败的升级任务并执行以下任一操作：

- 单击失败的升级任务旁边的“重试”
- 转至“选择操作”**>**“重试升级作业”

有关更多信息，请参阅 重试失败的升级作业。

[NSADM-93439]

安全性

更新现有 **API** 定义　在“安全”**>**“**API** 网关”**>**“**API** 发现”中，您现在可以使用选定的 API 资源更新现有 API 定义。

有关更多信息，请参阅 使用发现的 API 端点更新现有 API 定义。

[NSADM-97433]

已修复的问题

在 2023 年 8 月 9 日的内部版本中解决的问题。

预配

- VMware vCenter（基础结构 **>** 实例 **> Citrix ADC > VPX >** 预配）上的 NetScaler VPX 预配失败，因为之前删除的 VPX 实例使用的名称相同。

  [NSHELP-35983]

样书

- 当您尝试在“应用程序”**>**“配置”**>**“配置包”**>**“迁移 **ADC**”**>**“入门”**>**“指定配置”中将 ADC 配置从源 ADC 实例迁移到目标实例，单击下一步时，会间歇性地显示以下错误消息：

  未找到工作。

  [NSADM-97948]

- 如果您根据具有身份验证虚拟服务器和内置缓存策略绑定的样书定义创建 configpack，然后删除了 configpack，则删除成功。但是，如果您尝试使用相同的参数再次创建 configpack，则会出现以下错误消息：

  资源已存在。

  [NSHELP-35646]

2023 年 **7** 月 **26** 日

分析

支持配置通过样书将指标从 **NetScaler** 导出到 **Prometheus**　要将指标从 NetScaler 导出到 Prometheus，您必须在 NetScaler 中创建分析配置文件并指定体系结构文件。有关更多信息，请参阅使用 Pro metheus 监视 NetScaler 控制台、应用和应用安全。

在“应用程序”**>**“配置”**>**“样书”**>**“默认样书”中，您现在可以使用 **Prometheus TimeSeries Analytics** 配置样书并将配置运行到所有托管实例。

欲了解更多信息，请参阅 Prometheus 分析样书。

[NSADM-97698]

从 **NetScaler** 控制台为托管的 **NetScaler** 实例分配网络配置文件　当您在 NetScaler 控制台中启用虚拟服务器分析时，来自 NetScaler 的 AppFlow 数据将通过 NetScaler 子网 IP 地址 (SNIP) 导出到 NetScaler 控制台。在某些情况下，SNIP 可能会因为网络中的防火墙而被阻止。在这种情况下，您可能需要使用与 SNIP 不同的 IP 地址。有关网络配置文件的更多信息，请参阅使用指定的源 IP 进行后端通信。

现在，您可以通过 NetScaler 控制台将网络配置文件分配给 NetScaler 实例。导航到 基础结构 **>** 实例 **> Citrix ADC**，选择实例，然后从“选择操作”列表中单击“配置网络配置文件”为该实例分配网络配置文件。

> 注意：
>
> 在为实例分配网络配置文件之前，请确保已在所有虚拟服务器中禁用分析。

通过此增强功能，您可以分配网络配置文件以将 AppFlow 数据从 NetScaler 导出到 NetScaler 控制台。

[NSADM-91836]

基础结构

改善了使用 **CLI** 将 **NetScaler** 代理配置为代理时的用户体验　当您尝试将 NetScaler 代理注册到 NetScaler 控制台服务时，CLI 现在会提示您输入有关代理使用情况的（是/n）问题。

如果需要，您还可以选择在同一脚本中配置代理。

[NSADM-96921]

CLI 支持在注册 **NetScaler** 代理时查看端点 **URL**　在 NetScaler 控制台服务中注册 NetScaler 代理时，在 CLI 中输入服务 URL 后，您可以查看必须允许访问的所有端点 URL 的列表。

[NSADM-96920]

样书

支持样书分析中的其他属性　样书分析部分现已增强为：

- 接受参数以配置传输模式 (`transport-mode`)
- 为不同类型的流量配置 HDX Insight (`enable-hdxinsight-for`)
  - 启用 HTTP X-Forwarded-For 选项 (`http-x-forwarded-for`)
  - 启用客户端测量 (`client-side-measurements`)

有关更多信息，请参阅样书分析。

[NSADM-97839]

2023 年 **7** 月 **18** 日

管理和监视

支持 **CVE-2023-3519**、**CVE-2023-3466** 和 **CVE-2023-3467** 的识别和修复　NetScaler 控制台安全公告现在支持识别和修复 CVE-2023-3519、CVE-2023-3466 和 CVE-2023-3467。

识别：

- CVE-2023-3519 需要版本扫描和配置扫描的组合。
- CVE-2023-3466 和 CVE-2023-3467 需要进行版本扫描。

CVE-2023-3519、CVE-2023-3466 和 CVE-2023-3467 的修复需要将易受攻击的 NetScaler 实例升级到具有修复程序的版本和版本。

> 注意：
>
> 安全公告不支持已到达生命周期已结束 (EOL) 状态的 NetScaler 版本。我们建议您升级到 NetScaler 支持的内部版本或版本。

有关如何使用 NetScaler 控制台升级 NetScaler 实例的更多信息，请参阅使用作业升级 NetScaler 实例。

有关如何修复 CVE-2023-3519、CVE-2023-3466 和 CVE-2023-3467 的更多信息，请参阅安全公告。

> 注意：
>
> 安全公告系统扫描可能需要几个小时才能得出结论，并在安全公告模块中反映 CVE-2023-3519、CVE-2023-3466 和 CVE-2023-3467 的影响。要更快地查看影响，可以单击“立即扫描”开始按需扫描。

[NSADM-100103]

2023 年 **7** 月 **12** 日

已修复的问题

2023 年 7 月 12 日在 Build 中解决的问题。

- 当您备份或恢复 NetScaler 实例时，不会备份 `/var/metrics_conf` 目录。

  [NSHELP-35724]

- 当样书定义中包含 `operations` 部分时，配置包的部署可能会失败。

  [NSHELP-35588]

2023 年 **7** 月 **3** 日

分析

配置作业 **-** 支持创建用于配置指标从 **NetScaler** 导出到 **Prometheus** 的作业　要将指标从 NetScaler 导出到 Prometheus，您必须在 NetScaler 中创建分析配置文件并指定体系结构文件。有关更多信息，请参阅使用 Prometheus 监视 NetScaler、应用程序和应用程序安全。

在配置作业中，您现在可以使用内置模板中的 `NSConfigurePrometheusAnalyticsProfile` 模板创建作业，指定所需的参数，然后在所有托管实例上运行该作业。

有关详细信息，请参阅安排一项任务，配置指标从 NetScaler 导出到 Prometheus。

[NSADM-97251]

基础结构

NetScaler 代理缓存 **NetScaler** 镜像　由于 NetScaler 映像在下载后会缓存在 NetScaler 代理中，因此 NetScaler 升级所需的时间现在已大大缩短了。因此，后续的升级任务无需下载映像。

> 注意：
>
> 这仅适用于使用 NetScaler 代理添加的 NetScaler。

有关更多信息，请参阅 创建 ADC 升级作业。

[NSADM-76343]

已修复的问题

- 在 Web Insight 中，当您向下钻取任何指标以查看详细信息，然后进一步向下钻取任何指标时，图表将保留在先前的视图中，但所有其他详细信息均按预期显示。

  因此，这就形成了一种假设，即进一步的向下钻取没有按预期进行。

  [NSADM-98995]

- 当您尝试在“应用程序”**>**“配置”**>**“配置包”**>**“迁移 **ADC**”**>**“入门”**>**“指定配置”中将 ADC 配置从源 ADC 实例迁移到目标实例，单击下一步时，会间歇性地显示以下错误消息：

  “未找到作业”。

  [NSADM-97948，NSADM-97727]

- 在 应用程序控制板中，当您选择应用程序并导航到 **SSL** 选项卡以绑定证书时，会显示一条错误消息“在数据库中找不到证书”。

  [NSHELP-35654]

2023 年 **6** 月 **14** 日

安全性

支持在不选择端点的情况下创建 **API** 定义　在 安全 **> API** 网关 **> API** 发现 > 虚拟服务器 页面中，您现在可以在不选择端点的情况下创建 API 定义。单击“创建 **API** 定义”时，会出现一个弹出窗口，供您确认是否必须为所有已发现的端点创建 API 定义。单击“是”以创建包含所有端点的 API 定义，否则单击“否”。

有关更多信息，请参阅 发现 API 终端节点。

[NSADM-94318]

样书

在 **replace ()** 函数中支持其他参数类型 `replace()` 内置函数也可以接受以下内置类型的列表：

- `string`
- `ipaddress`
- `tcp-port`
- `number`
- **`boolean`**

有关更多信息，请参阅 replace()。

[NSADM-96802]

已修复的问题

2023 年 6 月 14 日的内部版本中解决的问题。

- 在升级作业（基础结构 **>** 升级作业）中，选择升级前验证失败的实例并单击“重新验证”时，会显示一条错误消息。

  [NSADM-98329]

- 基础结构 **> Citrix ADC** 清单 **> Citrix ADC (MPX/VPX/CPX/BLX)** 页面缺少 MPX 实例。

  [NSHELP-35593]

- 当您从基础结构 **> SSL** 控制板 **> SSL** 证书 **>** 导出报告中到处每周、30 天或 90 天的 SSL 到期报告并选择表格时，生成的报告会显示一个空域列。

  [NSHELP-35592]

- 在 基础结构 **> SSL** 控制板 **> SSL** 证书中，NetScaler 高可用性对不显示主设备和辅助设备的“P”和“S”的上标。

  [NSHELP-35523]

- 在 NetScaler 版本 13.1 及更高版本中，在 NetScaler 升级期间不会执行 ISSU 命令。

  [NSHELP-35391]

- 对于群集中的多个群集 IP 地址 (CLIP)，当您在基础结构 **>** 实例 **> Citrix ADC >** 添加的方括号中添加 CLIP 时，配置将失败，并且 CLIP 无法添加到 NetScaler 控制台。

  [NSHELP-35323]

2023 年 **5** 月 **31** 日

分析

任务功能中的合并许可建议　在任务中，您现在可以查看池化许可授权的建议和“引导我”工作流程。作为管理员，这些合并许可建议可确保您充分利用 NetScaler 控制台的所有功能。

有关更多信息，请参阅查看建议并高效管理您的 ADC 和应用程序。

[NSADM-93988]

将 **SSL** 见解数据导出到 **Splunk** 和 **New Relic**　当您在“设置” **>** “生态系统集成”中创建将 Citrix ADM 与 Splunk 和 New Relic 集成的新订阅时，您现在可以选择 **SSL** 证书见解选项。使用 **SSL** 证书洞察 选项配置订阅后，您可以在 Splunk 和 New Relic 控制板中查看 SSL 数据（SSL 虚拟服务器和 SSL 证书相关数据）。

有关更多信息，请参阅与 Splunk 集成和与 New Relic 集成。

[NSADM-92047]

已修复的问题

2023 年 5 月 31 日的内部版本中解决的问题。

- 在网关 **> HDX Insight >** 实例中，当您选择一个实例并导出数据时，桌面用户的用户名信息不可用。应用此修复后，用户名信息也可以在报告中找到。

  [NSADM-96024]

- 当您在基础结构 **>** 实例 **> Citrix ADC > SDX** 中选择为 SDX 实例配置 **SNMP** 时，会显示一条错误消息。如果将 SDX 配置文件配置为 SNMP v3 和 **NoAuthNoPriv** 作为安全级别，则会出现此问题。

  [NSHELP-35324]

- 在基础结构 **>** 配置 **>** 配置作业 **>** 创建作业 **>** 选择配置中，当您输入密码变量 ($password$) 并保留类型为文本字段而不是密码字段，然后单击下一步时，页面无法加载。

  [NSHELP-35266]

- 在 Web Insight 中，当您使用快照选项导出数据时，报表中的图表显示为空白。

  [NSHELP-35147]

- 在 HDX Insight 中看不到分析。即使重启 Citrix ADM，分析也仅在短时间内可见，稍后变为不可见。

  [NSHELP-35128]

- 对于基础结构 **>** 实例 **> Citrix ADC > SDX >** 控制板中的 SDX 实例，当资源的已用值和可用值为零时，系统资源利用率图表会显示空白和空白值字段。

修复后，如果已用值和空闲值为零，则资源名称旁边会显示数字零。

[NSHELP-35069]

2023 年 5 月 18 日

分析

支持从 **Web Insight** 中的每个控件中导出　在 **Web Insight** 中，导出选项现已引入到所有小部件中，它使您能够以表格格式导出数据。使用此增强功能，您可以：

- 从任何控件中单独导出所需的数据。
- 深入分析任何指标，还可以从任何小部件导出所需的数据。

早些时候，出口数据仅提供合并报告。

> 注意
>
> 您也可以继续使用现有的“导出”选项来生成合并报告。

[NSADM-94140]

基础结构

查看完整的证书链　现在，您可以查看证书的完整链接链，包括中间证书，直至根 CA 证书。

要查看证书链，请导航到基础结构 **> SSL** 控制板，选择 SSL 证书并单击详细信息。

[NSADM-52467]

支持记录事件，无论事件时间长短　NetScaler 控制台现在允许您记录所有事件，无论您在事件规则中设置的事件时长如何。

要设置此选项，请导航到基础结构 **>** 规则 **>** 添加 **>** 配置事件时长，然后选中“无论事件持续时间长短立即记录事件”复选框。

[NSHELP-19914]

已修复的问题

2023 年 5 月 18 日的内部版本中解决的问题。

- 在基础结构 **>** 升级作业 **>** 添加 **>** 计划任务中，如果您选择高可用性中的节点执行两阶段升级，并在两个“开始时间”字段中选择相同的时间，则继续操作时会出现以下错误消息：

  “common.date_diff_error: 升级时间之间应该有至少 1 小时的差异”

  即使您更改了字段中的开始时间，“创建作业”选项卡也会显示一个空页面。

  [NSHELP-35016]

- 在基础结构 **>** 实例公告 **>** 升级建议中，版本 13.0 的维护结束 (EOM) 和生命周期结束 (EOL) 详细信息不正确。

  [NSHELP-34953]

- 任何事件的电子邮件警报都错误地显示了该区域。通过此修复，该区域不会显示在事件的电子邮件警报中。

  [NSHELP-34913]

2023 年 **5** 月 **9** 日

管理和监视

支持识别和修复 **CVE-2023-24488** 和 **CVE-2023-24487** NetScaler 控制台安全公告现在支持识别和修复 CVE-2023-24488 和 CVE-2023-24487。

识别：

- CVE-2023-24488 需要同时进行版本和配置扫描。
- CVE-2023-24487 需要进行版本扫描。

CVE-2023-24487 和 CVE-2023-24488 的修复需要将易受攻击的 ADC 实例升级到已修复的发行版和版本。

有关 CVE-2023-24487 和 CVE-2023-24488 的固定版本详细信息的更多信息，请参阅 安全公告。

> 注意：
>
> ADC 版本 13.1—45.63 取代了构建 13.1—45.61。

有关如何使用 NetScaler 控制台升级 ADC 实例的 详细信息，请参阅创建 ADC 升级任务。

> 注意：
>
> 安全公告系统扫描可能需要几个小时才能得出结论并在安全公告模块中反映 CVE-2023-24488 和 CVE-2023-24487 的影响。要更快地查看影响，可以单击“立即扫描”开始按需扫描。

[NSADM-93570]

2023 年 **4** 月 **25** 日

2023 年 4 月 25 日版本中提供的增强和变更。

分析

Web Insight-支持在图表中查看零值　在 **Web Insight** 中，当您深入研究应用程序、客户端、URL 或实例下的任何指标时，分析视图现在可以在所选时长内提供图表中零值（例如 0 毫秒和 0 个请求）的可见性。

早些时候，如果在选定的时间内没有收到任何流量或事务，Web Insight 会跳过这些 nil 值来显示图表。作为管理员，您现在可以查看包含这些 nil 值的完整图表。

[NSADM-88686]

样书

指定用户组对配置包的访问权限　作为管理员，您现在可以限制用户组访问其他用户组创建的配置包。要选择此选项，请导航到设置 **>** 用户和角色 **>** 组 **>** 授权设置 **>** 配置包 **>** 用户组创建的所有配置。

[NSADM-92374]

已修复的问题

2023 年 4 月 25 日的内部版本中解决的问题。

- 在 应用程序 **>** 配置 **>** 配置包中，当您使用 属性 **>** 显示键的搜索条件输入搜索查询时，会显示搜索结果，但搜索栏会显示结果的索引号。

  修复后，搜索栏以文本而不是数字显示搜索查询。

  [NSADM-96859]

分析

- **HDX Insight** 和 **Gateway Insight** 中的带宽数据以每秒字节数而不是每秒位数显示不正确。

  [NSHELP-34836]

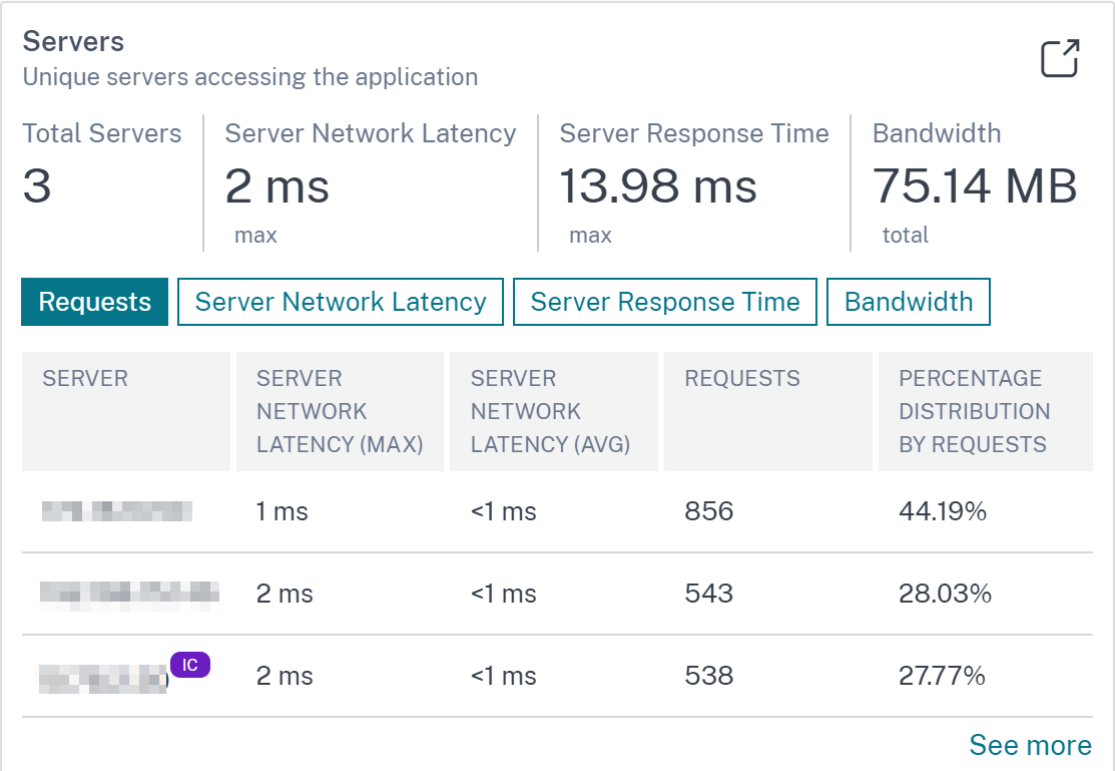
2023 年 **4** 月 **13** 日

2023 年 4 月 13 日版本中提供的增强和更改。

分析

Web Insight 中的集成缓存通知　在 NetScaler 实例中启用集成缓存后，无需往返原始服务器即可处理符合条件的请求。在 **Web Insight** 中，这些集成缓存请求当前显示在具有虚拟 服务器 IP 地址的服务器下方，而不是实际的服务器 IP 地址。

为了更好地了解这些集成缓存请求，您现在可以在“服务器”下的 ADC 虚拟服务器 IP 地址旁边查看 IC 通知。



对于未使用集成缓存处理的请求，实际的源服务器 IP 地址是可见的。

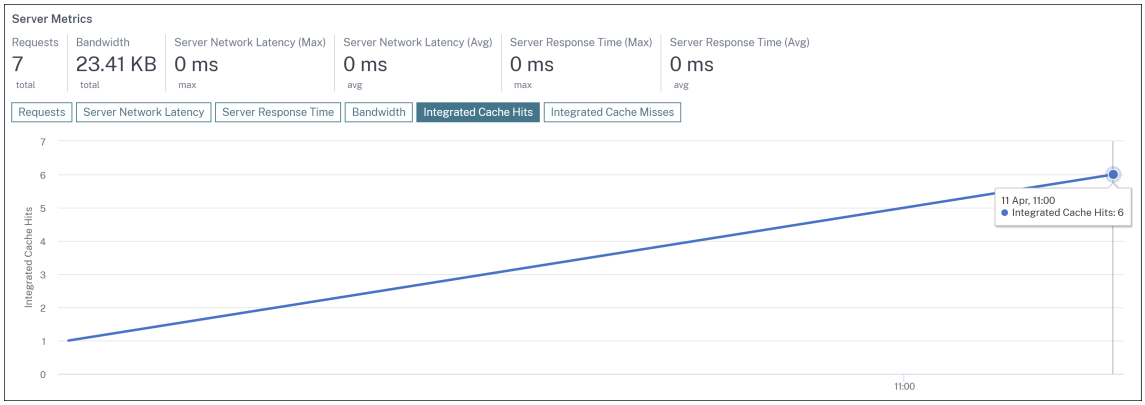
作为管理员，此通知使您能够快速识别 ADC 实例是否已处理集成缓存请求。

[NSADM-91864]

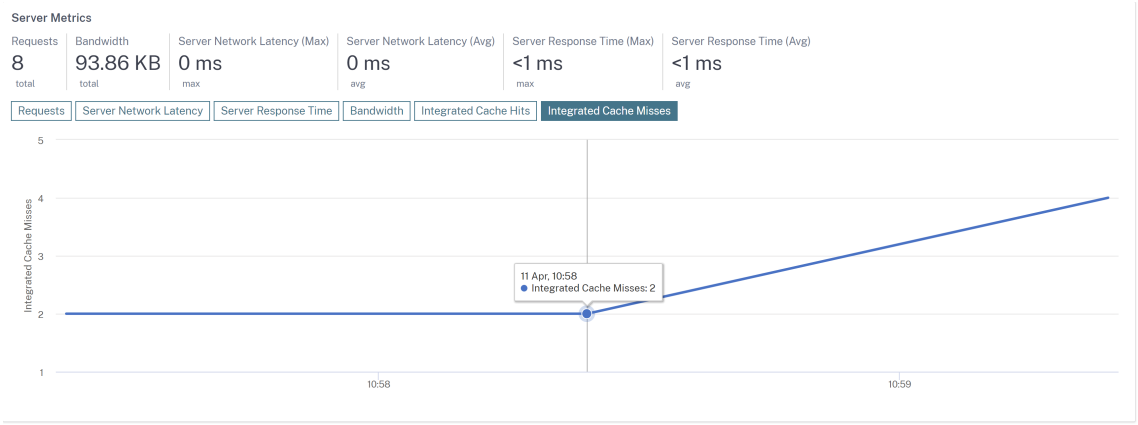
Web Insight 中的集成缓存命中率和未命中率图　在 **Web Insight** 中，当您深入查看服务器时，服务器指标 现在会显示“集成缓存命 中数”和“集成缓存未命中”选项卡。

作为管理员，图表视图位于：

- 在集成缓存命中率选项卡中，您可以查看 NetScaler 设备从缓存中提供的响应总数。



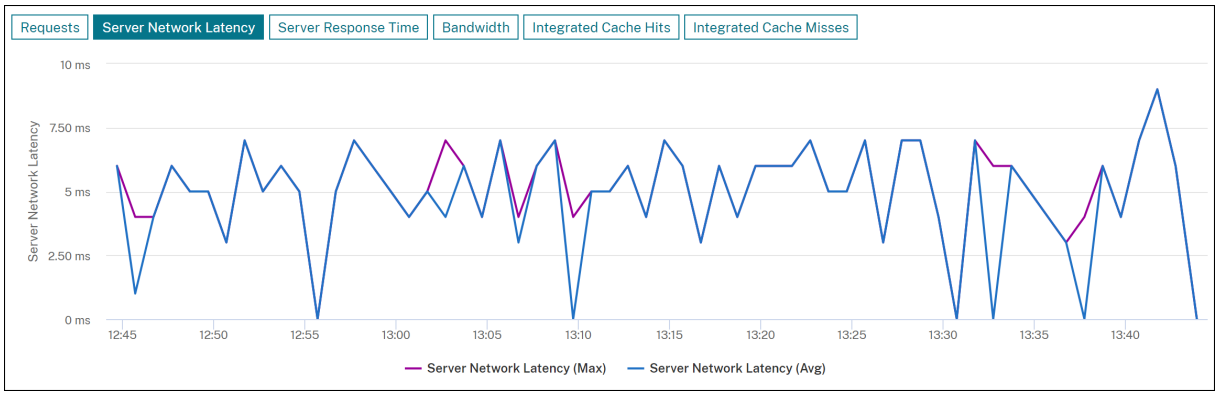
- 在集成缓存未命中选项卡中，您可以查看 NetScaler 设备从源服务器提供的响应总数。



[NSADM-93952]

Web Insight-查看图表中的平均值和最大值　从 13.1 45.47 或更高版本开始，支持 NetScaler 控制台中的 **Web Insight**，可以在服务器和客户端下显示最大延迟值。

除此支持外，当您深入查看服务器或客户端时，现在可以在摘要面板中查看平均值和最大值，也可以将鼠标指针悬停在服务器网络延迟、服务器响应时间和客户端网络延迟中的时间序列分析图上。



作为管理员，此增强功能使您能够在所选持续时间内在图表中直观显示最大延迟。

[NSADM-93816]

基础结构

在 **NetScaler** 控制台 **GUI** 中查看数据存储趋势　在 设置 **>** 数据存储管理中，您现在可以查看当前部署中不同功能的数据存储信息。数据存储管理 控制板可帮助您可视化数据的存储方式以及功能是否在其存储权限内运行。

> 注意

> 预计在即将发布的版本中，数据存储政策将发生变化。通过这些更改，在历史数据超过存储限制后，您将无法存储历史数据。

有关更多信息，请参阅 管理数据存储。

[NSADM-94623]

已修复的问题

2023 年 4 月 12 日的内部版本中解决的问题。

基础结构

- 在高可用性部署中，无法选择仅将构建映像文件上载到辅助节点。

  作为修复的一部分，您现在可以从基础结构 **>** 升级作业 > 创建任务选项卡 > 仅上载到辅助节点，将构建映像文件上载到辅助节点。

  [NSADM-96079]

- 从 基础结构 **>** 实例 **> NetScaler** 导出的报告不显示辅助节点的序列号。

  现在，报告显示 NetScaler 实例的主节点和辅助节点的序列号。您还可以查看 基础结构 **> NetScaler** 清单中的报告。

  [NSHELP-18816]

2023 年 **4** 月 **5** 日

2023 年 4 月 5 日版本中提供的增强和更改。

安全性

在 **NetScaler** 控制台 **GUI** 中根据发现的 **API** 端点创建 **API** 定义　现在，您可以在“安全” **>** “**API** 网关” **>** “**API** 发现”中从发现的 **API** 端点创建 **API** 定义。

[NSADM-85957]

统一控制板**-**查看 **API** 分析的关键指标　现在，在统一控制面板（概述 **>** 控制面板）中，您可以查看通过 NetScaler 控制台配置的 API 端点的关键指标。

有关更多信息，请参阅用于查看实例关键指标详细信息的统一控制板。

[NSADM-85954]

已修复的问题

2023 年 4 月 5 日的内部版本中解决的问题。

- 以下页面将显示“证书文件”和“密钥文件”字段的“选择设备”选项：
  - 基础结构 **>** **SSL** 控制板 **>** 管理证书存储 **>** 添加
  - 基础结构 **>** **SSL** 控制板 **>** **SSL** 证书 **>** 更新

  修复后，“选择设备”选项现已删除。

  [NSHELP-34566]
- 如果 NetScaler 使用本地 NetScaler 控制台作为许可服务器，并且 在基础架构 **>** 实例 **>** 代理中修改了代理，则会出现以下问题：

  `The IP address of the license server on NetScaler changes from the IP address of the on-premises NetScaler Console to the IP address of one of the NetScaler agents`。

  [NSHELP-34483]
- 当您从基础结构 **>** 实例 **>** **NetScaler** **>** **SDX** 选项卡 **>** 配置文件中编辑使用 SNMPv3 配置的 SDX 管理员配置文件的密码时，会出现以下错误消息：

  `Please provide valid authentication protocol. The possible values are MD5, SHA`。

  [NSHELP-34372]

2023 年 **3** 月 **14** 日

已修复的问题

2023 年 3 月 14 日的内部版本中解决了以下问题：

在基础结构 **>** **SSL** 控制板 **>** 安装证书中，当您上载与现有证书链具有相同根证书的证书链时，证书安装会失败。以下文本显示在基础结构 **>** **SSL** 控制板 **>** **SSL** 审核日志 **>** 设备日志 **>** 命令日志中：

```
Resource Already Exists
```

[NSHELP-34233]

当您从“设置”**>**“通知”**>**“电子邮件”中删除电子邮件通讯组列表时，会出现以下错误：

```
Error: Bad Gateway
```

出现此问题的原因是电子邮件通讯组列表的名称有空格。

作为修复的一部分，NetScaler 控制台现在允许您删除带有空格的邮件分发列表。

[NSHELP-34545]

2023 年 3 月 2 日

分析

Web Insight 的改进功能　在 Web Insight 中，您现在可以在应用程序指标下查看以下增强功能：

- 引入了新的摘要选项卡，使您可以直观地了解应用程序性能的概述，例如响应时间、请求和带宽。作为管理员，这使您能够深入了解所选持续时间内的应用程序性能。可以使用切换选项自定义视图。
- 在请求选项卡中，除了现有的请求总数外，您还可以根据请求总数查看来自前 5 个客户端的请求。作为管理员，这使您能够深入了解在选定时段内访问应用程序的客户端。
- 在带宽选项卡中，您可以根据总带宽消耗量查看前 5 台服务器的带宽消耗。作为管理员，这使您能够深入了解在选定时长内消耗更多带宽的服务器。
- 在响应时间选项卡中，您还可以在同一图表上查看客户端网络延迟、服务器网络延迟和服务器处理时间。作为管理员，这使您能够深入了解客户端、服务器和应用程序在选定持续时间内发生的延迟。可以使用切换选项自定义视图。

  [NSADM-87792]

基础结构

删除非活动的 **NetScaler** 控制台 **Express** 帐户　如果您的 NetScaler 控制台 Express 帐户在 45 天内处于非活动状态，则该帐户将被删除。Citrix 会在处于非活动状态 30 天后发送提醒。

[NSADM-93203]

管理和监视

NetScaler 高可用性升级的执行摘要变更　在 NetScaler 控制台 GUI 中，基础架构 > 升级作业 **>** 执行摘要中的执行摘要不再显示与高可用性同步相关的命令。

这是因为，在 NetScaler 高可用性升级期间，如果 NetScaler 主节点和辅助节点处于不同的版本，NetScaler 会禁用节点之间的高可用性同步。NetScaler 控制台不执行此操作。

[NSADM-93441]

在网络报告中为单个实体设置阈值　在基础结构 **>** 网络报告 **>** 阈值中，您现在可以在配置阈值时为特定实体设置阈值。

有关详细信息，请参阅 网络报告。

[NSADM-91727]

支持安排单个代理升级　在 基础架构 > 实例 > 代理 > 设置中，您现在可以安排每个 NetScaler 代理的升级。您可以选择自动将代理升级到下一个版本，也可以指定时间和时区来安排升级。

有关更多信息，请参阅 代理升级设置。

[NSADM-91719]

NetScaler 实例升级方面的改进功能　升级前验证选项卡中现在提供以下更改：

- 禁止升级的实例部分 - 此新部分列出了由于升级前验证错误而被阻止升级的实例。
- 快速清理按钮 - 此按钮在“磁盘空间详细信息”窗格中可用，可让您快速释放多个文件夹中的磁盘空间。

有关更多信息，请参阅 如何升级 ADC 实例。

[NSADM-91505]

NetScaler BLX 映像现已在映像库中可用　从基础结构 > 升级作业 > 升级 **NetScaler BLX** > 选择映像升级 NetScaler BLX 时，您现在可以从图像库中选择 **NetScaler BLX** 映像。

[NSADM-86864]

安全性

查看 **NetScaler** 实例的 **NetScaler Web App Firewall** 版本和机器人签名　现在，您可以查看 NetScaler 实例的 NetScaler Web App Firewall 版本和机器人签名。最新的签名版本保护您的实例免受 CVE 的侵害。有关更多信息，请参阅签名警报文章和机器人签名警报文章。

[NSADM-92378]

应用程序性能分析

Web Insight 的改进功能　在 **Web Insight** 中，您现在可以在服务器和客户端中查看最大网络延迟值。作为管理员，此增强功能使您能够确定以最大延迟运行的确切服务器或客户端。

早些时候，Web Insight 仅根据所有服务器和客户端的平均延迟值提供最大值。

[NSADM-91834]

其他

在统一控制板中创建和应用过滤器　在统一控制板（概述 > 控制板）中，您现在可以在以下位置创建和应用过滤器：

- 应用程序

- ADC 基础结构
- 应用程序安全性

作为管理员，您只能应用筛选器并查看所选实例或应用程序的见解。

有关更多信息，请参阅用于查看实例关键指标详细信息的统一控制板。

[NSADM-91873]

已修复的问题

2023 年 3 月 2 日的内部版本中解决的问题。

- 在基础结构 **>** 升级作业中，当您选择已完成的作业，该作业的升级前或升级后脚本文件名带有特殊字符，然后从“选择操作”列表中下载输出脚本时，将显示“找不到文件”错误消息。

[NSHELP-33854]

2023 年 **2** 月 **7** 日

分析

安全违规显示 **OWASP** 标签　在 NetScaler 控制台 GUI 中，安全违规现在会显示 OWASP 标签。它支持 OWASP 2017 和 OWASP 2021 列表。这些标签可以帮助您确定违规行为是否属于 OWASP 前 10 名列表。

选择违规行为以查看更多详细信息。现在，详细信息包括 OWASP 2017 和 OWASP 2021 列。这些列显示了 OWASP 代码，您可以使用这些代码从 OWASP Web 站点上了解有关违规行为的更多信息。

[NSADM-92999]

管理和监视

支持在没有当前密码的情况下更改代理密码　作为超级管理员，您现在可以允许在不使用当前密码的情况下更改代理密码。

导航到“设置”>“全局设置”**>**“系统配置”>“代理和时区”**>**“代理”，然后选中“删除更改代理密码的当前密码必备条件”复选框。更改代理密码页面将不再包含“当前密码”字段。

要再次显示“当前密码”字段，请清除“删除代理密码更改的当前密码必备条件”复选框。

[NSADM-91826]

修订了 **NetScaler** 控制台 **Express** 帐户的时间序列数据可视化间隔　对于使用 Express 帐户管理的虚拟服务器，现已修订了过去 **1** 小时持续时间的分析图表和网络报告图表中的时序数据可视化。

功能	现有数据可视化时间间隔	新的数据可视化时间间隔
“应用程序”控制板	1 分钟	5 分钟
网络报告	5 分钟	10 分钟
Web Insight、HDX Insight、Gateway Insight、Security Insight、BOT Insight、详细事务	1 分钟	5 分钟

[NSADM-93200]

已修复的问题

2023 年 2 月 7 日的内部版本中解决了以下问题。

当您启用或禁用 ADC 实例的系统日志设置时，ADM 不会在 ADC 实例中保存配置。因此，配置更改事件不会保存在 NetScaler 控制台中。

[NSHELP-33264]

在基础结构 **>** 实例 **>** 代理中，安装带有密码加密密钥的 SSL 证书后，端口 443 上与代理的连接将失败。

[NSHELP-33614]

2023 年 **1** 月 **24** 日

已修复的问题

2023 年 1 月 24 日的内部版本中解决了以下问题。

当您从 NetScaler 控制台 GUI 导航到 基础架构 > 实例 > NetScaler > SDX > 选择操作 **>** 配置 **SNMP**，在 **NetScaler SDX** 实例上启用 **SNMP** v3 时，会出现错误消息。

[NSHELP-33852]

2023 年 **1** 月 **10** 日

管理和监视

使用“引导我”工作流程查看建议并将您的 **ADC** 和应用程序作为可操作的任务进行高效管理　在 NetScaler 控制台 GUI 中，引入了一个新的任务选项，您现在可以在其中查看基于订阅和当前使用情况的建议。作为管理员，您可以：

- 将待办事项任务视为有关许可、分析、事件、SSL 证书等的可操作建议
- 使用引导我选项完成任务，该选项提供了成功完成任务的指导工具提示
- 确认任务并将它们移至存档
- 转到存档任务，使用指导工具提示来解决经常出现的需求

这些建议可确保您利用 NetScaler 控制台的所有功能，启用产品发现和产品推荐的功能，以便高效管理部署。

有关更多信息，请参阅查看建议并高效管理您的 ADC 和应用程序。

[NSADM-68719]

样书

在样书配置 **GUI** 中启用或禁用网络掩码长度　当您从样书创建具有 `type: ipnetwork` 属性的配置包时，样书配置 GUI 现在会在 **IP** 地址 字段旁边显示 网络掩码长度 按钮。

您可以执行以下操作之一：

- 启用可输入网络掩码长度
- 禁用可输入网络掩码 IP 地址

[NSADM-80696]

2022 年 **12** 月 **13** 日

管理和监视

支持 **CVE-2022-27518** 的识别和修复　NetScaler 控制台安全公告现在支持识别和修复 CVE-2022-27518。

识别 CVE-2022-27518 需要将版本扫描和配置扫描相结合，而修复需要将易受攻击的 ADC 实例升级到具有修复程序的版本和版本。

有关如何修复 CVE-2022-27518 的更多信息，请参阅安全公告。

> 注意
>
> 安全公告系统扫描可能需要几个小时才能得出结论，并在安全公告模块中反映 CVE-2022-27518 的影响。要更快地查看影响，可以单击“立即扫描”开始按需扫描。

2022 年 **12** 月 **9** 日

分析

停止高级许可 **ADC** 实例的高级安全分析　NetScaler 控制台不再 支持高级许可的 ADC 实例的高级安全 分析。通过此次升级，在 NetScaler 控制台 GUI 中：

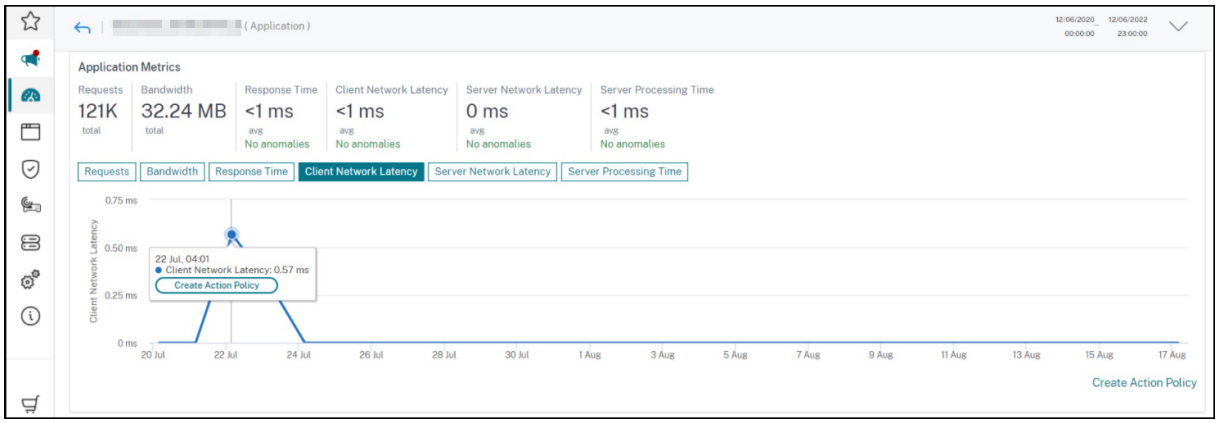
- 高级安全分析中的现有配置和相关的基于行为的违规行为现在不可见。
- 其他机器人和 WAF 违规行为的可见性保持不变。有关更多信息，请参阅违规类别。
- 只有违反 WAF 和机器人时才支持 Splunk 和 New Relic 导出。

[NSADM-92342]

从 **Web Insight** 配置操作策略　在 **Web Insight** 中，您现在可以根据图表趋势为以下指标配置操作策略：

- 客户端网络延迟
- 服务器网络延迟
- 服务器处理时间

作为管理员，当您发现任何异常流量模式或任何应用程序的这些指标突然出现峰值时，此增强功能允许您在将相对操作策略置于图表中的特定点后单击“创建操作策略”来创建相对操作策略。



[NSADM-88682]

操作策略 **-** 添加多个应用程序　现在，当您为客户端网络延迟、服务器网络延迟和服务器处理时间配置操作策略时，可以使用 **IN** 运算符选择多个应用程序并将其应用到单个策略中。

有关更多信息，请参阅操作策略。

[NSADM-88680]

2022 年 **11** 月 **29** 日

基础结构

NetScaler 控制台中显示的 **Z** 许可证到期信息　现在，您可以导航到 基础架构 > 池化许可 **>** 池化容量 **Z** 许可，在 **NetScaler** 控制台中查看 **MPX** 和 **SDX** 实例的 **Z** 许可到期信息。

[NSADM-80202]

管理和监视

NetScaler 控制台中已停止的 **SD-WAN** 和 **HAProxy** 功能　NetScaler 控制台不再支持 SD-WAN 和 HAProxy 功能。因此，适用于 SD-WAN 和 HAProxy 的相关功能现在在 NetScaler 控制台 GUI 中不可用。

[NSADM-90549]

SDX 升级改进-支持从资源库中选择 **SDX** 图像　现在，当您在 NetScaler 控制台中安排维护任务以升级 SDX 实例时，您可以选择从升级所需的映像库中进行选择。导航到 基础结构 **>** 升级作业 **>** 创建作业，选择 升级 **NetScaler SDX**，然后单击 继续 升级 SDX 实例。

[NSADM-88832]

已修复的问题

2022 年 11 月 29 日的内部版本中解决的问题。

- 如果管理员在 ADM 之前将来自 Azure AD 的用户添加到 DaaS 或其他 NetScaler 产品中，则无法登录 ADM。

  [NSHELP-32556]

- 在 基础结构 **>** 网络功能 **>** 负载平衡 **>** 服务中，即使在 ADC 实例上配置的服务总数超过 5000，配置的服务总数也仅显示 5000 个计数。

  [NSHELP-32299]

2022 年 **11** 月 **16** 日

分析

与 **New Relic** 集成　现在，您可以将 NetScaler 控制台与 New Relic 集成，在 New Relic 控制面板中查看 WAF、机器人和基于行为的违规行为的分析。通过这种集成，您可以：

- 在 New Relic 控制板中合并所有其他外部数据源
- 集中查看分析情况

NetScaler 控制台收集机器人、WAF 和基于行为的事件，并根据您的选择实时或定期将其发送到 New Relic。作为管理员，您还可以在 New Relic 控制板中查看机器人、WAF 和其他基于行为的事件。

有关更多信息，请参阅与 New Relic 集成。

[NSADM-83119]

基础结构

AutoScale 组的自动升级　AutoScale 组的升级操作现已自动化。导航到 基础结构 **>** 公有云 **> AutoScale** 组，然后选择要升级的 AutoScale 组。NetScaler 控制台执行所需的检查并升级 Autoscale 组。

有关更多信息，请参阅修改 AutoScale 组。

[NSADM-84955]

管理和监视

ADM 服务网络报告控制板上提供加密利用率指标　现在，您可以在“网络报告”控制板中添加和查看加密利用率指标。导航到 基础结构 **>** 网络报告 **>** 创建控制板。选择 **SSL** 加密利用率 作为实体，然后为网络报告创建控制板。

[NSADM-88416]

已修复的问题

2022 年 11 月 16 日的内部版本中解决的问题。

现在，在 NetScaler 控制台 GUI 中，非对称加密单位和对称加密单位是可编辑字段。在配备了 Intel Coleto (COL) 芯片的 NetScaler SDX 设备上配置 NetScaler VPX 实例时，您可以输入 ASU 和 SCU 的数量。

导航到基础架构 > 实例 > **NetScaler**，然后在 **SDX** 选项卡上，选择要在其中配置 NetScaler VPX 实例的 SDX 实例。在“选择操作”中，选择“配置 **VPX**”，然后在显示的页面中，在“加密 分配”下输入加密容量

[NSHELP-33297]

2022 年 **11** 月 **8** 日

管理和监视

支持 **CVE-2022-27510**、**CVE-2022-27513** 和 **CVE-2022-27516** 的识别和修复　NetScaler 控制台安全公告现在支持识别和修复三种新 CVE：CVE-2022-27510、CVE-2022-27513 和 CVE-2022-27516。

- 识别 CVE-2022-27510 需要将配置扫描和版本扫描相结合，修复需要将易受攻击的 ADC 实例升级到已修复的版本和版本。
- 识别 CVE-2022-27513 需要将配置扫描和版本扫描相结合，修复需要将易受攻击的 ADC 实例升级到已修复的版本和版本。
- 识别 CVE-2022-27516 需要将配置扫描和版本扫描相结合，修复需要将易受攻击的 ADC 实例升级到已修复的版本和版本。

有关如何修复 CVE-2022-27510、CVE-2022-27513 和 CVE-2022-27516 的更多信息，请参阅安全公告。

> 注意
>
> 安全公告系统扫描可能需要几个小时才能得出结论并反映安全公告模块中 CVE-2022-27510、CVE-2022-27513 和 CVE-2022-27516 的影响。要更快地查看影响，可以单击“立即扫描”开始按需扫描。

该公告还发布了一篇关于 HTTP 请求走私攻击的安全文章。有关 HTTP 请求走私攻击的信息，请参阅 CTX472830。

> 注意
>
> NetScaler 控制台安全公告仅支持识别和修复 CVE。它不支持“安全”文章中强调的安全问题。因此，我们不支持识别和修复 HTTP 请求走私攻击。

[NSADM-88525]

2022 年 **10** 月 **28** 日

基础结构

为代理升级指定时区　在 基础结构 **>** 实例 **>** 代理 **>** 设置 **>** 升级中，开始时间使用您在 全局设置 **>** 系统配置中选择的时区。

有关设置时区的更多信息，请参阅 设置 NetScaler 控制台时区。

[NSADM-88417]

已修复的问题

2022 年 10 月 28 日的内部版本中解决的问题。

在“设置”**>**“许可和分析配置”**>**“配置分析”中，当您应用以下筛选器时，“所有虚拟服务器”页面上的结果将消失：

- 名称
- 状态
- 类型

[NSHELP-32807]

当您配置第二个 NIC 以隔离对 NetScaler 控制台的管理访问时，第二个 NIC IP 地址被错误地分配给了与主 NIC 相同的 IP 地址。

[NSHELP-32567]

2022 年 10 月 12 日

分析

WAF 安全违规**-**查看命令注入语法分析　在 **WAF** 下的“安全”**>**“安全违规”中，您现在可以查看 命令注入语法 违规的日志和分析。有关详细信息，请参阅：

- HTML 命令注入保护检查
- 安全违规

[NSADM-85792]

基础结构

使用其他权限验证您的云访问配置文件　连接到 AWS 的 AutoScale 组的现有云访问配置文件需要额外的 IAM 权限。目前，由于缺少权限，NetScaler 控制台服务使云访问配置文件失效。要验证 IAM 权限，请执行以下操作：

1. 复制 创建 IAM 角色中提到的最新 IAM权限。
2. 转到 AWS 控制台，使用最新的 IAM 权限验证云访问配置文件的角色。

[NSADM-90096]

2022 年 9 月 27 日

分析

WAF 安全违规**-**查看屏蔽关键字的分析　在 **WAF** 下的“安全”**>**“安全违规”中，您现在可以查看屏蔽关键字和 **JSON** 区块关键字 违规的日志和分析。

有关详细信息，请参阅：

- 为 HTML 有效负载提供自定义关键字支持
- 安全违规

[NSADM-86225]

在白金 **ADC** 实例上配置机器人管理　在 NetScaler 控制台中，您现在可以：

- 配置机器人检测技术，并使用高级许可证将其部署到版本 13.0 36.27 或更高版本的 ADC 实例上。
- 通过样书或直接从 ADC 实例为配置了机器人检测技术的现有虚拟服务器启用机器人安全违规选项，查看机器人分析。

除了现有的样书配置外，此增强功能还进一步简化了配置机器人检测技术和在 ADC 实例上部署的过程。

有关更多信息，请参阅 在 NetScaler 控制台中配置机器人检测技术。

[NSADM-80413]

基础结构

为 **AutoScale** 应用程序创建配置作业的新选项　在 **AutoScale** 组 **>** 配置中，您现在可以通过选择 AutoScale 应用程序导航到配置作业。在 Cre **ate Job** 页面中，根据所选应用程序的配置详细信息显示示例命令。您可以编辑值或命令。另外，添加或删除命令。

> 注意
>
> 只能对使用 ADC CLI 命令模式创建的应用程序使用配置作业。

有关更多信息，请参阅 使用配置作业部署 AutoScale 应用程序。

[NSADM-85939]

当发生不可预见的事件时，**NetScaler** 控制台会重新安排作业　有时，在运行配置或升级任务时，您可能会遇到如下事件：

- NetScaler 控制台服务的升级正在进行中。
- 一个 ADM 代理出现故障。如果代理升级正在进行中，则可能会发生这种情况。

在这种情况下，NetScaler 控制台会将任务重新安排到接下来的一个小时。

早些时候，NetScaler 控制台无法识别 ADM 服务升级或代理状态。结果，超时后作业失败。

[NSADM-85554]

查看非托管 **CICO ADC** 实例的使用情况和许可证信息　现在，您可以导航到 基础结构 **>** 池化许可 **>** 带宽许可证 **> CICO** 以查看 ADM 服务上非托管 CICO ADC 实例的使用情况和许可证信息。

[NSADM-85452]

管理和监视

为辅助 **ADC** 实例生成技术支持包　在 ADC 高可用性对中，您现在也可以通过 ADM GUI 为辅助节点生成技术支持包。以前，您只能为主节点生成技术支持包。

[NSADM-88905]

查看当月每一天的网络报告数据点　在 基础结构 **>** 网络报告中，当您在控制板中选择一个月的持续时间时，它会显示每天的数据点。早些时候，它显示了每周的数据点。

[NSADM-88875]

样书

样书支持 **NetScaler BLX** 实例　在创建配置包时，您现在可以选择 NetScaler BLX 实例作为目标实例。早些时候，样书支持 NetScaler MPX、SDX、VPX 和 CPX 实例。

[NSADM-86253]

2022 年 **9** 月 **13** 日

样书

改进了配置负载平衡虚拟服务器的默认样书　借助改进的默认样书，您现在可以在 ADC 中为负载平衡虚拟服务器配置所有支持的选项。例如，您现在可以设置 IP 模式、IP 掩码、IP 范围等。以前，您只能在样书中配置较少的选项。我们在 NetScaler 控制台中添加了以下样书及其改进版本：

名称	版本
lb	2.0
lb-mon	2.0

[NSADM-80663]

已修复的问题

2022 年 9 月 13 日的内部版本中解决的问题。

- 在通过选择 Azure AD 作为身份提供者来邀请 IAM 组时，如果 ADM 角色有空格，则不会显示在“自定义访问权限”下。

  [NSHELP-32557]

- 如果管理员在 ADM 之前将来自 Azure AD 的用户添加到 DaaS 或其他 NetScaler 产品中，则无法登录 ADM。

  [NSHELP-32556]

2022 年 8 月 29 日

为 **NetScaler Gateway** 网关自动启用 **Gateway Insight** 和帐户接管

现在，所有获得许可的 NetScaler Gateway 虚拟服务器自动启用 **NetScaler Gateway** 的帐户接管和 **Gateway Insight**。在 NetScaler 控制台中，这使您能够查看以下方面的见解：

- 安全 **>** 安全违规中针对 NetScaler Gateway 的帐户接管攻击。NetScaler Gateway 登录页面的可用性成为恶意机器人窃取用户凭据并执行诸如凭据填充和密码喷洒之类的网络攻击的容易目标。作为管理员，您可能需要分析恶意机器人是否试图接管 NetScaler Gateway 帐户。有关更多信息，请参阅 NetScaler Gateway 的帐户接管。
- 与网关 **> Gateway Insight** 中的 NetScaler Gateway 虚拟服务器相关的问题。作为管理员，您可能需要监视网关实例以了解用户登录活动、登录失败原因、活跃用户、可用用户、机器人攻击等见解。有关更多信息，请参阅 Gateway Insight。

> 注意
>
> 自动启用 NetScaler Gateway 功能的 Gateway Insight 和“帐户接管”功能将分阶段向客户发布。
>
> - 您的 NetScaler 控制台必须配置一个或多个外部 NetScaler 代理，并且必须有一台或多台高级或高级网关设备。
> - 在您的 NetScaler 控制台中发布此功能后，所有获得许可的现有 NetScaler Gateway 虚拟服务器和后续获得许可的 NetScaler Gateway 虚拟服务器将自动为 NetScaler Gateway 启用 Gateway Insight 和帐户接管。
> - 对于所有使用 Gateway Insight 选项手动禁用的 NetScaler Gateway 虚拟服务器，不会自动为这些虚拟服务器启用 Gateway Insight。
> - 要禁用 **Gateway Insight** 选项，请执行以下操作：
>
>   1. 导航到 **Settings**（设置）**> Licensing & Analytics Configuration**（许可和分析配置）。
>   2. 在“虚拟服务器分析摘要”下，单击“配置分析”。
>   3. 在“所有虚拟服务器”页面中，选择 NetScaler Gateway 虚拟服务器，然后单击“编辑分析”。
>   4. 取消选择“**Gateway Insight**”选项，然后单击“保存”。
>
> - 禁用 **Gateway Insight** 选项后，**NetScaler Gateway** 的帐户接管将自动禁用。

[NSADM-82732]

统一控制板的改进

概述 **>** 控制板中的统一控制板 现已添加，其中包含每个类别下所有关键指标的小部件。当您单击“编辑控制板”时，您可以：

- 移除整个小部件（应用程序、ADC 基础结构、网关或应用程序安全）。
- 移除每个控件下方的较小部件。
- 单击“添加组件”，然后在每个组件下选择要查看的所需关键指标。

此增强功能使您能够通过在每个类别下添加或删除所需的组件来自定义控制板视图。

[NSADM-86337]

从所选地区中选择一个国家

当您首次登录 NetScaler 控制台服务时，您现在可以选择适合您业务需求的国家/地区。将根据您选择的地区显示国家/地区。以前，您只能选择区域。

例如，如果您选择 欧洲、中东和非洲 地区，GUI 会列出以下国家：

- 法国
- 英国
- 德国

同样，您可以从其他地区选择合适的国家。

[NSADM-83643]

Web Insight-查看密码相关问题的详细信息

在“应用程序”**>** “**Web Insight**”的“**SSL** 错误”下，您现在可以深入查看“密码不匹配”以查看详细信息，例如 SSL 密码名称、建议操作以及受影响应用程序和客户端的详细信息。

有关更多信息，请参阅 Web Insight。

SNMP 版本 **3** 支持 **ADM** 上的 **SDX** 配置

现在，您可以通过 ADM GUI 为 NetScaler SDX 实例创建 SNMP v3 配置文件。导航到 基础结构 **>** 实例 **> NetScaler > SDX** 选项卡，然后单击 配置文件。您可以添加所有配置文件参数，选择 **v3** 作为 SNMP 配置文件类型，然后单击“创建”创建 NetScaler SDX 配置文件。

[NSADM-84828]

2022 年 **8** 月 **16** 日

分析

应用程序控制板-查看详细见解以解决应用程序问题　在应用程序控制板中，当您深入查看应用程序时，您现在可以查看以下应用程序问题的 建议操作，从而查看详细见解以解决问题：

- 响应时间
- 活动服务
- 服务器不稳定
- 服务摆动

有关更多信息，请参阅 绩效指标（问题）。

[NSADM-84811]

基础结构

支持 **ADM** 代理的 **NIC** 卡　您可以在 ADM 代理上配置另一个 NIC 来管理对 NetScaler 控制台的访问。使用双 NIC 体系结构，ADM 代理现在能够：

- 在 ADM 代理和 ADC 实例之间建立通信
- 在 ADM 代理和 ADM 服务之间建立通信

有关更多信息，请参阅 NetScaler 控制台上的双 NIC 卡支持。

[NSADM-85781]

重新创建属于 **Google Cloud AutoScale** 组的群集　要查看属于 Google Cloud (GCP) AutoScale 组的 ADC 群集并对其进行故障排除，您现在可以导航到 基础结构 **>** 公有云 **> AutoScale** 组，然后单击查看群集。

您可以选择 **GCP** 群集，然后单击“重新创建”以删除现有群集并将其替换为新群集。所有应用程序配置都转移到新的 ADC 群集。

有关更多信息，请参阅 查看 ADC 群集并对其进行故障排除。

[NSADM-75731]

管理和监视

在统一控制板中查看 **ADM** 代理详情　在统一控制板中，您现在可以可视化 ADM 代理详细信息的概述。在“概述”**>** “控制板”中的“**ADM** 代理状态”旁边，您可以查看可用/不可用的代理。

单击“查看详细信息”可视化 ADM 代理详细信息的概述，例如内置代理总数、外部代理总数、代理 IP、状态、系统使用情况、诊断检查等。

有关更多信息，请参阅 统一控制板概述。

[NSADM-83096]

已修复的问题

- 启用分析或编辑从 HA 对配置的 NetScaler Gateway 虚拟服务器的分析后，高级设置（可选）下的 实例级别选项 将显示为禁用，即使启用了这些选项。

  [NSHELP-32188]

- 在 **Gateway > HDX Insight >** 用户中，当您选择用户时，ADM 不显示所选用户的详细信息，而是显示所有用户的详细信息。

  [NSHELP-32181]

- 在“网关”**>** “**HDX Insight**” **>** “实例”中，当您单击某个国家/地区以深入了解更多详细信息时，不会显示“当前会话”下的数据。

  [NSHELP-32125]

2022 年 **7** 月 **13** 日

管理和监视

支持 **CVE-2022-27509** 的识别和补救　NetScaler 控制台安全公告现在支持识别和修复 CVE-2022-27509。

识别 CVE-2022-27509 需要将版本扫描和自定义扫描相结合，而修复需要将易受攻击的 ADC 实例升级到已修复的版本和版本。如果您的易受攻击的 ADC 实例已将 `/etc/httpd.conf` 文件复制到 `/nsconfig` 目录中，请在计划 ADC 升级之前参阅 [自定义 ADC 配置的升级注意事项。

您也可以选择退出这些安全公告自定义扫描。有关自定义扫描设置和选择退出自定义扫描的更多信息，请参阅“安全公告”页面上的“配置自定义扫描设置”部分。

有关 ADM 如何识别易受 CVE-2022-27509 影响的 ADC 以及补救步骤的更多信息，请参阅 识别和修复 CVE-2022-27509 的漏洞。

> 注意
>
> 安全公告系统扫描可能需要几个小时才能得出结论并反思 CVE-2022-27509 对安全公告模块的影响。要更快地看到影响，您可以单击“立即扫描”开始按需扫描。

[NSADM-85549]

配置升级作业的访问策略　作为超级管理员，您现在可以配置访问策略，设置升级任务的权限（查看/编辑），并将该策略应用于您的 NetScaler 控制台用户。在“设置”**>** “用户和角色”**>** “访问策略”中，单击“添加”，通过选择“权限”下的“基础结构”**>** “升级作业”来配置访问策略。

有关更多信息，请参阅 在 NetScaler 控制台上配置访问策略。

[NSADM-82494]

支持在共享模式下在 **NetScaler BLX** 实例中进行配置审核　现在，您可以使用某些配置创建配置审核模板，并在共享模式下监视 NetScaler BLX 实例中的配置更改。有关详细信息，请参阅 创建审核模板。

[NSADM-82323]

在 **Web** 事务分析中支持 **CSV** 格式和计划导出　在 **Web** 事务分析中，当您单击“导出”图标时，您现在可以查看以下增强功能：

- 在“立即导出”中，可以以 CSV 格式导出数据。
- 引入了“计划导出”选项，使您可以通过电子邮件和 Slack 计划并以 CSV 格式导出数据。

有关更多信息，请参阅 Web 事务分析。

已修复的问题

在 NetScaler 控制台服务中，当您导航 到基础架构 **>** 实例 代理，然后 单击“****** 设置”以更改代理升级设置时，设置更改后会显示一条确认 ****** 消息“修改了代理升级 设置”。

[NSHELP-32099]

2022 年 **6** 月 **29** 日

应用程序

配置一个应用程序并将其与多个自定义应用程序关联　在 应用程序控制板中，您现在可以配置应用程序并将其与多个自定义应用程序关联。使用此功能，您可以对多个自定义应用程序重复使用同一个应用程序，而不必为每个自定义应用程序创建单独的应用程序。

有关更多信息，请参阅 配置应用程序并将其与多个自定义应用程序关联。

[NSADM-82040]

管理和监视

支持访问 **NetScaler** 控制台 **GUI** 的浏览器　NetScaler 控制台 GUI 现在只能从以下兼容浏览器版本中访问：

Web 浏览器	版本
Microsoft Edge	79 及更高版本
Google Chrome	51 及更高版本
Safari	10 及更高版本

Web 浏览器	版本
Mozilla Firefox	52 及更高版本

[NSADM-83943]

2022 年 6 月 15 日

基础结构

监视 **NetScaler** 代理系统参数的使用情况，并使用自我修复守护程序修复问题　NetScaler 代理现在通过在后台自动运行自我修复守护程序来监视其系统资源（CPU、内存和磁盘）。在以下情况下，自我修复守护程序会检查阈值并自动应用操作：

- 如果在特定持续时间内磁盘使用率超过 80% 或更多，则将应用清理空间（日志、备份日志、核心文件、崩溃文件等）操作来回收磁盘空间。
- 如果在特定持续时间内内存和 CPU 使用率超过 90% 或更多，则重新启动 ADM 进程以回收 CPU 和内存。

> 注意
>
> 自我修复守护程序不监视在 基础结构 > 实例 > 代理 > 设置 > 通知中配置的阈值。

[NSADM-82558]

2022 年 6 月 7 日

分析

查看自定义应用程序的机器人和 **WAF** 分析　在“安全”>“安全违规”中的 **WAF** 和机器人下，您现在可以选择自定义应用程序并查看适用于自定义应用程序的合并应用程序详细信息。您还可以从列表中选择一个应用程序并查看该自定义应用程序的特定应用程序的详细信息。

有关更多信息，请参阅 安全违规。

[NSADM-77375]

管理和监视

通过证书存储区导入和安装 **SSL** 证书包（含证书链）　在 基础结构 > **SSL** 控制板中，当您从“设置”旁边的可用列表中选择“管理证书存储”时，您可以：

- 单击“导入 **ADC** 证书”**>**“开始轮询”，SSL 证书包以及将服务器证书与其颁发者（中间 CA）链接的证书链从 ADC 实例导入到证书存储区。
- 在证书存储区中查看证书，选择一个证书，然后单击“安装”，在选定的 ADC 实例上安装证书和证书链。

[NSADM-82727]

NetScaler BLX 实例的升级支持　在基础结构 **>** 升级作业中，您现在可以创建作业来升级 NetScaler BLX 实例。您必须选择适当的构建映像（适用于 Ubuntu 或 Red Hat）才能成功升级。有关更多信息，请参阅 维护作业。

[NSADM-82324]

已修复的问题

在“基础结构”**>**“事件摘要”**>**“系统日志消息”中，仅显示过去 30 天的数据。通过此修复，数据最多可显示 180 天。

[NSHELP-30961]

2022 年 **5** 月 **10** 日

分析

将实时数据导出到 **Splunk**　现在，NetScaler 控制台与 Splunk 的集成使您能够将实时数据导出到 Splunk。在 ADM GUI 中，当您选择 实时导出选项并进行配置时，NetScaler 控制台中选定的违规行为将立即推 送到 Splunk。

有关更多信息，请参阅 与 Splunk 集成。

[NSADM-84529]

WAF 学习引擎的改进　在 NetScaler 控制台中，您现在可以配置学习配置文件并部署或跳过以下额外安全检查的放松规则：

- **JSON SQL**
- **JSON** 命令注入
- **JSON XSS**

> 注意
>
> 要使用这些安全检查配置学习配置文件，NetScaler 实例必须为 13.1—14.10 或更高版本。

有关更多信息，请参阅 WAF 学习引擎。

[NSADM-80921]

应用程序

统一控制板的改进　概述 **>** 控制板中的统一控制板 现在允许您根据自己的选择对其进行自定义。使用“编辑控制板”选项，您可以：

- 拖动小部件
- 移除小部件
- 添加小部件
- 重置为默认值

进行更改后，单击“保存”。

> 注意
>
> 默认情况下，显示所有小部件。如果您自定义了控制板，保存了更改并使用了“重置为默认值”选项，则上次保存的自定义控制板将恢复。

[NSADM-52144]

基础结构

对 **ADM GUI** 的改进　现在，您可以单独展开或折叠 ADM GUI 导航菜单。这种改进使您能够查看每个部分中的所有选项。

[NSADM-85480]

支持 **CVE-2022-27507** 和 **CVE-2022-22508** 的识别和补救　NetScaler 控制台安全公告现在支持识别和修复两个新的 CVE：**CVE-2022-27507** 和 **CVE-2022-22508**。

- 识别 **CVE-2022-27507** 需要将版本扫描和配置扫描相结合，而修复需要将易受攻击的 ADC 实例升级到已修复的版本和版本。

  ADM 安全公告不支持缓解措施。如果您已对 ADC 实例应用缓解措施（临时解决方法），则在您完成修复之前，ADM 仍会将 ADC 识别为易受攻击。

  对于 **CVE-2022-27507**，即使您应用了缓解措施并暂时禁用了 EDT 流量的 HDX Insight（参阅安全公告），在您完成修复（升级到版本和拥有修复）后，ADM 安全公告仍会将 ADC 识别为漏洞。

- 识别 **CVE-2022-27508** 需要将版本扫描和配置扫描相结合，而修复需要将易受攻击的 ADC 实例升级到已修复的版本和版本。

  有关如何修复 CVE-2022-27507 和 CVE-2022-22508 的更多信息，请参阅安全公告。

> 注意
>
> 安全公告系统扫描可能需要几个小时才能得出结论，并在安全建议模块中反映 **CVE-2022-27507** 和 **CVE-2022-27508** 的影响。要更快地看到影响，您可以单击“立即扫描”开始按需扫描。

[NSADM-85673]

已修复的问题

在 基础结构 **>** 实例 **> NetScaler** 中，当您更改管理员配置文件密码并在密码中包含% 时，将显示一条错误消息。

[NSHELP-31392]

2022 年 **4** 月 **27** 日

管理和监视

使用正确的 **ns.conf** 文件通过 **ADM GUI** 降级 **ADC** 在 基础结构 **>** 升级任务中，当您创建升级任务以将 ADC 实例升级到较低版本时，ADM 现在会选择兼容 `ns.conf` 文件，从中将配置应用于 ADC 实例。所选 `ns.conf` 文件的版本必须相同或低于用户选择的版本。如果 ADC 实例中没有合适的 `ns.conf` 文件，则不允许降级并显示相应的错误消息。

[NSADM-81421]

已修复的问题

- 启用高级安全分析，应用包含一个或多个基于行为的违规行为的配置文件，然后单击“保存”时，表中的详细信息不会显示在“设置”**>**“许可和分析配置”**>**“所有虚拟服务器”中。

  注意：基于行为的违规行为包括过多的客户端连接、异常大的上载事务、异常大的下载事务和异常高的请求速率。

  [NSADM-85020]

- 在“基础结构”**>**“事件摘要”**>**“系统日志消息”中，仅显示过去 30 天的数据。通过此修复，数据最多可显示 180 天。

  [NSHELP-30961]

2022 年 **4** 月 **12** 日

分析

针对限制速率的机器人违规行为添加了新的违规行为 速率限制规则检测来自同一客户端的多个请求。在“安全”**>**“安全违规”**>**“应用程序概述”中的“机器人”下，您现在可以查看以下违规详细信息：

- **URL**
- 源 **IP**
- 地理位置
- 会话

单击“日志”可查看时间、客户端 IP、机器人类型、机器人检测等详细信息。有关更多信息，请参阅查看机器人违规详情。

[NSADM-80925]

在机器人违规中支持无头浏览器违规　在“安全”**>**“安全违规”**>**“应用程序概述”中的“机器人”下，您现在可以查看 **Headless Browser** 违规 的详细信息。单击“日志”可查看时间、客户端 IP、机器人类型、机器人检测等详细信息。

有关更多信息，请参阅查看机器人违规详情。

[NSADM-89027]

管理和监视

CVE-2022-21827 不在 **NetScaler** 控制台安全公告的范围内　CVE-2022-21827 会影响 21.9.1.2 之前支持的 Windows 版本的 NetScaler Gateway 插件。

NetScaler 控制台不支持检测和修复影响适用于 Windows 的 NetScaler Gateway 插件的漏洞。此外，无法通过在 ADC 端执行任何检查、验证 ADC 版本或检查 ADC 配置来评估 NetScaler Gateway 插件漏洞。此 CVE 的检测和修复只能根据客户端上部署的适用于 Windows 的 NetScaler Gateway 插件版本进行评估。

因此，对该漏洞的检测和修复超出了 NetScaler 控制台安全公告的范围。

有关更多信息，请参阅安全公告中不支持的 CVE。

在发送给客户的产品电子邮件中提供取消订阅选项　客户（新客户和非活跃客户）现在可以选择取消订阅 NetScaler 控制台发送的产品邮件中的所有电子邮件通知。有关订阅或取消订阅的更多信息，请参阅 电子邮件订阅。

[NSADM-83272]

在应用程序控制板中保留筛选器　在“应用程序”**>**“控制板”中，当您通过搜索栏和关键量度应用筛选器时，筛选器现在会被保留。即使出现以下情况，您也可以查看相同的筛选器：

- 您可以从 ADM GUI 中的其他导航栏返回到“应用程序”**>**“控制板”。
- 关闭浏览器并从同一个浏览器中打开一个新会话。

> 注意
>
> 如果您使用其他浏览器或以隐身模式打开新会话，则不会保留过滤器。

[NSADM-82038]

样书

自动更新配置包　在 NetScaler 控制台证书存储库中更新 SSL 证书时，与 SSL 证书关联的配置包会自动更新。

[NSADM-80694]

2022 年 **3** 月 **31** 日

分析

改进了安全违规中的高级安全分析　作为对高级安全分析功能的改进，现在简化了首先启用 高级安全分析，然后使用“设置”图标创建配置文件的过程。现在，您可以在单个工作流中启用 高级安全分析、创建配置文件并将配置文件分配给虚拟服务器。

有关更多信息，请参阅 启用高级安全分析。

[NSADM-81383]

统一控制板的改进　在“概述”**>**“控制板”中，您现在可以查看以下改进：

- 您可以单击所有类别下的关键指标计数以查看受影响的 ADC 实例/应用程序/网关的详细信息。
- 在“应用程序”下，在 SSL 密钥指标中对 GUI 进行了细微的更改，以显示更多信息。
- 在网关下，用户地理分布根据用户数量显示前 3 个国家/地区。

[NSADM-82758]

管理和监视

支持 **SSL** 控制板中的 **ECDSA** 算法　在 **SSL** 控制板 **>** 设置 **>** 企业策略中配置企业策略时，现在可以在 建议签名算法中选择 **ECDSA**。

有关 ECDSA 的更多信息，请参阅 ECDSA 密码套件支持。

有关企业策略配置的更多信息，请参阅 配置企业策略。

[NSADM-71321]

载入

ADM 对 **Kubernetes** 版本 **1.23** 的支持　NetScaler 控制台现在支持使用 Kubernetes 版本 1.23 添加和管理群集。

[NSADM-83683]

2022 年 **3** 月 **16** 日

载入

测试 **ADC** 实例的载入准备情况　当您想要使用默认内置代理选项将 ADC 实例载入 NetScaler 控制台时，可以执行测试运行以确保 ADC 实例已准备就绪，可以载入。有关更多信息，请参阅测试 ADC 实例的载入准备情况。

[NSADM-80502]

2022 年 **3** 月 **1** 日

管理和监视

从 **Azure AD** 邀请用户或组加入 **ADM**　作为超级管理员，您现在可以邀请用户或组从连接的 Azure AD 到 NetScaler 控制台加入 NetScaler 控制台。在执行此操作之前，请确保 Azure AD 已连接到 Citrix Cloud，请参阅将 Azure Active Directory 连接到 Citrix Cloud。以前，您只能使用 Citrix 身份邀请用户。

选择 Azure AD 作为身份提供者时，只能为选定的用户或组指定自定义访问权限。用户可以使用他们的 Azure AD 凭据登录 NetScaler 控制台。使用此功能，您无需为所选 Azure AD 的用户创建 Citrix 身份。如果用户被添加到受邀组，则无需向新添加的用户发送邀请。该用户可以使用 Azure AD 凭据访问 NetScaler 控制台。

[NSADM-81039]

上载到 **ADC** 的证书和密钥文件由 **ADM** 保存，信息存储在 **ADM** 数据库中　当您使用 ADM 服务 GUI 中的 **SSL** 控制板 将证书和密钥文件上载到证书存储区时，只有证书文件的元数据和加密内容保存在 ADM 数据库中。用于解密内容的密钥和密码保存在云钱包中。

[NSADM-72475]

ADM 中的新网络报告　以下新网络报告将添加为总计数器：

- 身份验证成功与失败
- **HTTP** 身份验证成功与失败
- 非 **HTTP** 身份验证成功与失败

- **AAA** 会话
- 当前 **AAA** 会话
- 当前 **ICAOnly** 会话
- 当前 **ICAOnly** 连接
- 当前的 **ICA (Smart Access)** 连接

您可以使用这些计数器来添加阈值和接收通知。有关更多信息，请参阅 网络报告。

[NSADM-62239]

操作策略 **-** 使用交易详细信息配置机器人和 **WAF** 通知　在操作策略中，配置操作策略时，现在可以选择每个客户端机器人违规和每个客户端 **WAF** 违规选项。这些选项使您能够配置和接收包含交易详细信息（例如客户端 IP、攻击总数、违规类型等）的通知。

有关更多信息，请参阅配置操作策略以接收应用程序事件通知。

[NSADM-80630]

选择退出“安全公告”自定义扫描　NetScaler Application Delivery Management 服务用户界面现在允许您选择退出安全公告自定义扫描。当您选择退出这些安全公告自定义扫描时，将不会在安全公告中评估需要自定义扫描的 CVE 对您的 ADC 实例的影响。

要选择退出“安全公告自定义扫描”，请参阅 自定义扫描设置。

[NSADM-80288]

样书

在样书描述和标题中使用 **HTML** 格式化标签　在 样书 定义中，您现在可以添加标题字段并为文本使用 HTML 格式标记。您也可以将图像作为标题的一部分，图像将在配置表单的顶部呈现。此功能允许您为样书用户添加信息图表，以帮助理解样书配置。如果您在标题中使用图像，请确保在 `image` 标记中使用 base64 编码的图像格式。

```
name: app-stylebook-with-HTML-tags
namespace: com.examples.stylebooks
version: `1.0`
display-name: `Example App StyleBook`
header: 'This <b> StyleBook </b> defines all the app configuration for
    <i>Load Balanced Application </i>. The following image describes the
     target deployment for the app <img id=`b64img` src=`data:image/png;
    base64,` />'
```

[NSADM-80699]

交付位于 **ADC** 实例虚拟网络或 **VPC** 之外的 **AutoScale** 应用程序　当应用程序服务器和 ADC 实例位于不同的虚拟网络、VPC 网络和子网上时，请提供您拥有应用程序服务器的子网或 VPC 的 CIDR 块。配置配置参数时，在“源服务器”字段中指定 CIDR 块。通过这种方式，您可以从位于 ADC 实例虚拟网络或 VPC 网络之外的应用程序服务器交付应用程序。

以前，此功能仅适用于 AWS 中的 AutoScale 组，现在您也可以在 Azure 和 Google Cloud 中使用此功能。

有关详细信息，请参阅：

- Microsoft Azure。
- Google Cloud。

  [NSADM-78617]

2022 年 **2** 月 **10** 日

管理和监视

支持 **ShowConfiguration** 模板　在配置编辑器中，当您选择批处理配置时，现在可以使用 **ShowConfiguration** 模板。将 **ShowConfiguration** 模板拖到右窗格中，然后输入要在 NetScaler 实例上运行的 show 命令。

例如，您可以输入 `sh ns info`、`sh node`、`sh ns stats`、`sh interface` 和 `shell ls /var/tmp` 等命令并查看输出。

您可以将命令的输出作为文本文件下载。

[NSADM-66132]

配置操作策略以接收应用程序事件通知　除了现有的应用程序事件分析视图外，您还可以配置操作策略以通过 Slack、Email、PagerDuty 或 ServiceNow 获取应用程序事件通知。应用程序事件包括性能问题、机器人和 WAF 违规以及服务图违规。作为管理员，使用操作策略，您可以实时获取事件通知。

使用操作策略，您可以：

- 为应用程序事件预定义某些条件。
- 通过 Slack、Email、PagerDuty 和 ServiceNow 获取有关以下事件的通知：
  - **WAF SQL** 违规
  - **WAF XSS** 违规
  - **WAF** 推断 **XML** 违规

    > 注意

> 要收到 WAF 违规通知，最低违规交易量必须为 20%。例如，在 100 笔交易中，至少有 20 笔必须是违规交易。

- 前 **3** 名 **WAF** 违规行为

  （由 SQL、XSS 和 XML 造成的违规总数必须为 30%。例如，在 100 个事务中，30 个或更多事务必须是 SQL、XSS、Infer XML 违规行为的组合。）

- 机器人违规行为

  （有关机器人违规列表的更多信息，请参阅 违规类别。）

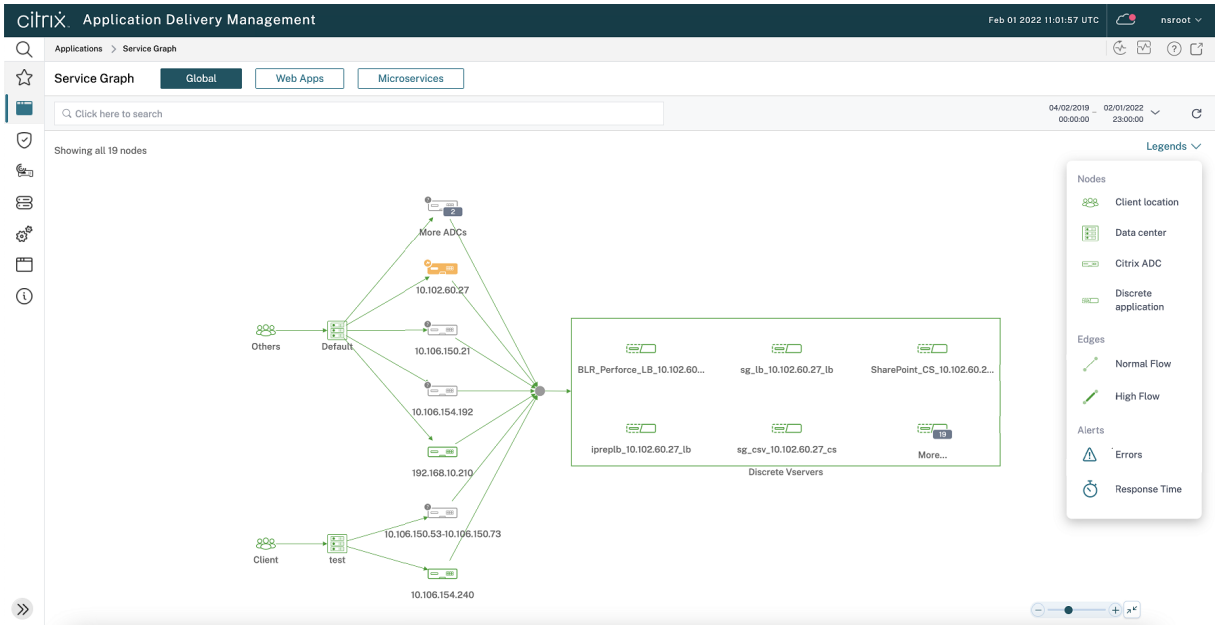
- 应用程序得分违规
- 客户端网络延迟
- 服务器网络延迟
- 服务器处理时间
- 服务图表违规

有关更多信息，请参阅配置操作策略以接收应用程序事件通知。

[NSADM-70968]、[NSADM-76588]、[NSADM-72799]

应用程序

服务图表的改进　在全局服务图和微服务服务图中，您现在可以查看提供服务图中可用符号描述的图例。



[NSADM-82077]

载入

为低接触式载入工作流程电子邮件配置设置　作为基于 ADM Service Connect 的低接触入门流程的一部分，您将收到来自 NetScaler 控制台服务的产品发起的电子邮件。您可以通过以下方式配置和管理在此工作流程中收到的电子邮件：

- 为所有管理员启用电子邮件
- 启用/禁用选定管理员的电子邮件
- 禁用所有管理员的电子邮件

有关配置和管理电子邮件的更多信息，请参阅 电子邮件设置。

[NSADM-80289]

查看 **NetScaler** 代理诊断信息并接收端点验证警报　NetScaler 控制台现在定期（每隔一小时）对 NetScaler 代理执行诊断检查，并提供以下信息：

- 端点可访问性
- 运行状况检查探测器
- 代理代理

如果代理端点的可访问性状态发生变化（从正常更改为需要审核），则超级管理员会收到一封包含问题详细信息的电子邮件通知。

有关更多信息，请参阅 查看代理诊断和接收端点验证警报。

[NSADM-69407]

样书

自动协调样书配置包的更新　有时，更新部署在 ADC 实例上的样书配置包可能与其部署状态有所不同。在这种情况下，配置包更新会失败。样书引擎现在会自动协调这些差异并更新配置包。之前，GUI 上出现了一条消息，需要您确认才能协调更改，然后才能更新配置包。

[NSADM-80660]

在 **ADM** 中管理数据源　在 NetScaler 控制台中定义数据源可帮助您在创建或更新样书配置时使用来自外部来源的数据作为输入。否则，您必须明确提供样书所需的每个输入。在 NetScaler 控制台中，您可以使用任何托管 ADC 实例作为样书配置输入的数据源。在 NetScaler 控制台中，您可以使用托管的 ADC 实例作为数据源。您还可以定义自定义数据源，这些数据源可以在创建或更新配置时用作输入。要查看自定义数据源，请转到 应用程序 **>** 配置 **>** 数据源。

使用样书定义中的 `datum` 内置类型来定义数据源。

示例：


```
parameters:
  -
    name: selected-lb
    label: Select an existing ADC
    type: datum
    required: true
    data-source:
      type: managed-adc
```

在此示例中，`datum` 参数用于定义 `managed-adc` 数据源。此数据源允许您从由 NetScaler 控制台管理的 ADC 实例检索数据。

[NSADM-80659]

检查配置包的样书兼容性　在 ADM GUI 中更改配置包的样书时，现在可以确定对新选择的样书定义所做的更改。以及这些更改如何影响配置包。有了这些信息，您可以在更改样书定义之前对其进行必要的更新。或者，您可以决定继续使用现有的样书。

例如，如果您更改配置包的样书，则现有样书可以具有允许的 HTTPS 端口，而新选择的样书可以有 SSL。在这种情况下，您可能还需要为 SSL 端口编辑相同的 HTTPS 值。

[NSADM-80664]

2022 年 **1** 月 **25** 日

ADC 低接触接入 **ADM** —查看自动诊断

以下信息仅适用于通过 ADM Service Connect 功能连接到 ADM 服务的 ADC 实例。

之前有一个使用诊断工具来解决低接触载入问题的手动流程。现在，您还可以在 ADM GUI 上查看有关在低接触载入时出现问题的 ADC 实例的诊断信息。

当您进入基于 ADM Service Connect 的低接触载入工作流程时，在资产清单页面中，您可以看到新添加的载入准备状态选项，该选项提供 ADC 实例的载入准备状态，例如“需要审查”或“确定”。

您也可以通过导航到 基础结构 **>** 实例 **> NetScaler** 并单击“资产清单”选项来查看此视图。

然后，您可以使用这些信息来了解和解决问题。

有关更多信息，请参阅 使用诊断工具或 ADM GUI 解决问题。

[NSADM-77245]

支持尚未使用 **Citrix Cloud** 的客户进行低接触登录培训

作为使用 ADM Service Connect 工作流程低接触启动 NetScaler 实例的一部分，尚未使用 Citrix Cloud 的客户现在可以注册 Citrix Cloud 并轻松地将其 ADC 实例载入 ADM 服务。这些客户将收到一封来自 NetScaler 控制台服务

的电子邮件，指导他们使用“加入 **ADM** 服务”。通过单击此按钮，他们可以注册 Citrix Cloud，并使用低接触式载入工作流程将其 ADC 实例载入 ADM 服务。有关更多信息，请参阅 使用服务连接对 NetScaler 实例进行低接触式启动。

[NSADM-76466]

基础结构分析-为特定问题配置通知

在 **Infracture Analytics** 中，您现在可以选择所需的问题，为超过配置阈值的问题启用通知，并仅接收选定问题的通知。早些时候，已收到有关所有问题的通知。此增强功能使您能够仅接收有关要监视的选定问题的通知。

有关更多信息，请参阅 配置通知。

[NSADM-76361]

2022 年 **1** 月 **17** 日

ADM 对 **BLX** 群集的支持

现在，您可以在 ADM 中添加 BLX 群集。在 ADM GUI 中，添加了群集 IP 地址 (CLIP)，现在可以在控制板中看到群集节点的计数。

[NSADM-78588]

用于查看实例关键指标详细信息的统一控制板

作为管理员，您现在可以可视化一个控制板，该控制板基于以下内容提供关键指标详细信息的概述：

- 应用程序
- ADC 基础结构
- 应用程序安全性
- 网关

这个单一窗格控制板使您能够查看详细信息，从而更好地监视实例使用情况和性能。有关更多信息，请参阅用于查看实例关键指标详细信息的统一控制板。

[NSADM-74075]

安全违规-**JSON SQL** 注入语法

在 **WAF** 下的“安全”**>**“安全违规”中，您现在可以查看所选应用程序的 **JSON SQL** 注入语法 违规。有关更多信息，请参阅 违规详情。

[NSADM-62909]

使用样书的保留关键字作为参数和表达式

现在，在样书定义中定义参数和表达式时，可以使用保留关键字。保留的关键字如下所示：

```
"and", "false", "in", "not", "true", "or"
```

例如，名为的参数现在 `not` 是有效的参数 (`$parameters.not`)。

[NSADM-80657]

样书支持嵌套参数条件

在样书定义中，您现在可以在参数条件中指定参数条件。这些条件称为嵌套参数条件，并使用 repeat 构造来定义这些条件。当您想要对列表参数的每个项目应用操作时，嵌套参数条件很有用。

示例：

```
parameters-conditions:
  -
    repeat: $parameters.lbvservers
    repeat-item: lbvserver
    parameters-conditions:
      -
        target: $lbvserver.port
        action: set-allowed-values
        condition: $lbvserver.protocol == "HTTPS"
        value: $parameters.ssl-ports
```

在此示例中，当用户为负载平衡虚拟服务器选择 HTTPS 协议时，将动态填充端口值。而且，它适用于列表中的每个负载平衡虚拟服务器。

有关更多信息，请参阅 嵌套参数条件。

[NSADM-62747]

已修复的问题

在 GSLB 设置中，当多个 ADC 实例使用相同的域名时，实体轮询会错误地更新数据库。

[NSHELP-29885]

已知问题

July 17, 2024

NetScaler 应用程序交付管理（NetScaler 控制台）存在以下已知问题：

管理和监视

在 基础架构 **>** **SSL** 控制面板 **>** 管理证书存储中，当您单击“导入 **NetScaler** 证书”时，NetScaler 控制台无法导入 PFX 格式的 NetScaler 证书。

[NSHELP-34803]

基础结构

- 当您尝试在 NetScaler BLX 实例上安装证书时，安装失败，并且基础结构 **>** **SSL** 控制板 **>** **SSL** 审核日志页面显示以下错误消息：

  ```
  SCP: Authentication by password fails on _<ip-address>_.
  ```

  [NSADM-102202]

- 当在基础架构 **>** 事件 **>** 规则 **>** 创建规则 **>** 选择失败对象中选择某些实体的情况下创建事件规则时，不会显示所有选定实体。当存在大量虚拟服务器、服务或服务组时，就会出现此问题。

  解决方法：请联系 NetScaler 支持团队以获取有关此问题的帮助。

  [NSADM-110553]

数据合规性

January 29, 2024

PCI DSS 合规性

支付卡行业 (PCI) 数据安全标准 (DSS) 是一项信用卡行业安全标准，它定义了存储、处理或传输信用卡数据时必须存在的人员、流程和技术所需的安全级别。PCI DSS 适用于商家、处理商和服务提供商，以及存储、处理或传输信用卡数据的所有其他实体。PCI DSS 合规性认证 (AOC) 最终是实体对需要且存在特定安全级别的证明。

NetScaler Application Delivery Management PCI DSS 合规性

NetScaler Application Delivery Management (ADM) 服务通过针对客户的 PCI DSS 合规性控制域进行评估，成功实现了 PCI DSS 合规性。NetScaler 控制台服务不存储、处理和/或传输客户 PCI 数据。NetScaler 控制台服务每年还将接受合格安全评估机构 (QSA) 的 PCI DSS 评估，以评估我们的服务和控制措施。

尽管 Citrix 帮助支持客户的 PCI DSS 合规性，但使用 NetScaler 产品和服务本身并不能实现 PCI DSS 合规性。客户有责任确保他们有足够的合规计划、内部流程和控制措施，以实现和维持其 PCI DSS 合规性要求。

单击 NetScaler 控制台服务 PCI 合规性认证 (AOC) 以下载离线报告。

NetScaler 遥测计划

September 2, 2024

NetScaler 遥测计划是一项必需的数据收集计划，它允许上载客户遵守维护和支持许可义务所需的许可和功能使用数据。Citrix 出于合法利益（包括许可合规性）收集基本许可遥测数据以及 NetScaler 部署和功能使用遥测数据。还收集 NetScaler 控制台配置和功能使用情况数据，以管理、衡量和改进 Citrix 产品和服务。
自 14.1-28.x 版本开始，NetScaler 遥测计划将自动启用。

> 备注：
>
> - 遥测上载每 24 小时自动进行一次。
> - 为了收集遥测指标并将其存储在您的 NetScaler 实例中，作为 2024 年 6 月 18 日发布的 NetScaler 遥测计划的一部分，通过 NetScaler 控制台将以下配置推送到您的 NetScaler 实例。

```
enable ns feature AppFlow
add analytics profile telemetry_metrics_profile -type timeseries -
    outputMode prometheus -metrics ENABLED -serveMode Pull -
    schemaFile "./telemetry_collect_ns_metrics_schema.json" -
    metricsExportFrequency 300
```

> - 使用以下网关遥测命令更新 `/nsconfig/.telemetry.conf` 文件。NetScaler 控制台每小时检查一次此命令，如果缺少此命令，则进行添加。此命令仅推送到具有 VPN 虚拟服务器配置的 NetScaler 实例：

```
ns_telemetry_server,<Console IP>,5140
```

> - 一些遥测参数是通过脚本收集的，这些脚本从 NetScaler 控制台推送到 NetScaler 实例。这些脚本是只读的，不会更改 NetScaler 中的任何内容。
> - 通过遥测收集的信息（例如电子邮件地址、用户名和 IP 地址）通过使用单向哈希算法在源头对信息进行哈希处理，从而安全地进行假名化。因此，Citrix 无法访问或读取这些值。此遥测数据仅用于逻辑资产匹配目的。

下表提供在 NetScaler 遥测计划中收集的参数详细信息：

类别	说明	我们用它做什么
许可证、NetScaler 部署和使用遥测	有关许可授权、分配、使用情况和高级别 NetScaler 部署数据以及 NetScaler 功能使用情况的信息。	许可证合规性以及管理、衡量和改进服务。
NetScaler 控制台部署和功能使用遥测	有关控制台部署和功能使用情况的信息。	管理、衡量和改进服务。

有关遥测参数列表的更多信息，请参阅数据治理。

数据治理

September 2, 2024

NetScaler 控制台服务是 Citrix Cloud 服务的一部分，它使用 Citrix Cloud 作为注册、入门、身份验证、管理和许可平台。作为 NetScaler 控制台服务的一部分，Citrix 收集数据并将其存储在 Citrix Cloud 中。本文档描述了收集的数据以及数据收集、存储和传输的方法。

有关 Citrix 数据保护实践的更多信息，请参阅 Citrix Cloud 服务数据保护概述。

此信息适用于安全官员、合规官员、信息审核员、网络基础架构和运营管理员以及业务线所有者。

NetScaler 遥测计划

自 **14.1-28.x** 版本开始在 NetScaler 控制台服务中启用 NetScaler 遥测计划。使用此程序，所需的数据会自动上载。有关收集到的所需遥测数据的更多信息，请参阅 NetScaler 遥测的数据治理。

我们如何收集、存储和传输数据

NetScaler 控制台服务从托管实例和代理收集数据。这些实例部署在客户场所，数据通过使用 TLS 1.2 协议加密的 SSL 通道安全地从代理（部署在客户场所）传输到云端。

数据存储在关系数据库中，在数据库层进行多租户数据隔离，并作为文件存储在托管在美国 AWS 云、EMEA（法兰克福）和 APJ（悉尼）中的 Elastic File System (EFS) 中，具体取决于客户选择的接入点 (POP)。所有 PoP 都托管在 AWS 商业区域。

密码、SNMP 社区字符串、SSL 证书和 NetScaler 配置备份使用每个租户的唯一的 AES 256 密钥进行加密，并安全地存储在数据库中。有关 Citrix Cloud 使用的商业区域以及 NetScaler 控制台服务在每个区域的存在情况的更多信息，请参阅地理注意事项。

数据类别

对于数据处理实践，数据分为：

- 客户内容 - 上载到客户帐户的任何数据或客户计算环境中的数据，NetScaler 有权访问这些数据来执行某些服务。
- 日志 -包括服务记录，包括但不限于：
  - 有关性能、稳定性、使用情况、安全性、支持的数据和信息
  - 有关设备、系统的技术信息

客户内容

NetScaler 控制台服务从各种来源收集信息：

- NetScaler
- NetScaler Gateway
- NetScaler Web App Firewall (WAF) 和机器人管理

除了日志中提及的信息外，NetScaler 控制台服务还收集有关管理员会话和活动细节的信息。

日志

日志用于便于提供软件更新、许可证身份验证、支持、分析和其他与 Citrix 用户协议一致的目的。

收集的元数据和遥测日志包括：

- NetScaler 服务代理虚拟机管理程序或公共云平台或同时使用代理虚拟机管理程序和公有云平台
- 代理地理位置
- NetScaler 版本
- NetScaler 产品类型
- 许可信息（快捷版和订阅版）
- NetScaler 控制台管理员使用云服务（从而改善管理用户体验）。

详细的客户内容和日志

- 事件管理（登录 **>** 基础架构 **>** 事件）
  - SNMP 陷阱提供有关 NetScaler 网络状态和性能的警报。

  - 遍历 NetScaler 网络状态信息的 Web 事务的系统日志。
  - 用于触发 SMS/Slack 事件通知的 SMS 服务器、Slack 和 PagerDuty 个人资料的详细信息。
  - 用于电子邮件配置的 SMTP 服务器详细信息。
  - 在 ServiceNow 中创建票证的 ServiceNow 配置文件详细信息。

- **SSL** 证书管理（登录 **>** 基础架构 **> SSL** 控制面板）
  - 由 NetScaler 实例优化的 Web 应用程序的 SSL 证书、SSL 密钥、SSL CSR、CA 颁发者和签名算法。
- 配置审核（登录 **>** 基础架构 **>** 配置 **>** 配置审核）
  - NetScaler 的数据跟踪配置审核与 NetScaler 实例相关的变更，包括 Web 应用程序服务器 IP 地址和 NetScaler IP 地址的详细信息。
- 配置作业（登录 **>** 基础架构 **>** 配置 **>** 配置作业）
  - NetScaler 配置详细信息、实例 IP 地址和 Web 应用程序服务器 IP 地址详细信息。
- 样书（登录 **>** 应用程序 **>** 配置 **>** 样书）
  - NetScaler 配置存储为模板，其中包括 Web 应用程序服务器 IP 地址的详细信息。
- 实例管理（登录 **>** 基础架构 **>** 实例）
  - NetScaler 实例的 IP 地址、NetScaler 实例类型、NetScaler 配置备份、NetScaler 关键事件以及部署 NetScaler 实例的数据中心的地理位置（如果已配置）。
- 基础架构分析（登录 **>** 基础架构 **>** 基础架构分析）
  - NetScaler 实例的 IP 地址、NetScaler 实例类型、NetScaler 关键事件、关联的应用程序数量以及部署 NetScaler 实例的数据中心的地理位置（如果已配置）。
- 应用程序（登录 **>** 应用程序）
  - 应用程序控制面板：应用程序 URL、请求方法、响应代码、总字节数、Web 应用程序服务器详细信息、虚拟服务器 IP 地址、客户端详细信息、浏览器、客户端操作系统、客户端设备、SSL 协议、SSL 密码强度、SSL 密钥强度、NetScaler 实例 IP 地址、服务器跳动的时间戳和响应内容类型。
- 分析（**AppFlow/Logstream**）
  - **Web Insight**（登录 **>** 应用程序）：虚拟服务器 IP 地址、客户端、URL、浏览器、操作系统、请求方法、响应状态、域、Web 应用程序服务器 IP 地址、SSL 证书、协商的 SSL 密码、SSL 密钥强度、SSL 协议和 SSL 故障前端。
  - **HDX Insight**（登录 **>** 网关）：ICA 用户详细信息、ICA 应用程序详细信息、VDA 服务器详细信息、HDX Insight 中的桌面详细信息、应用程序客户端的地理位置详细信息、HDX 活动会话详细信息、HDX 的 VPN 许可证、客户端 NetScaler IP 地址、客户端类型和版本。

  - **Gateway Insight**（登录 **>** 网关）：用户详细信息、应用程序详细信息、浏览器、操作系统、会话模式、网关许可证、AAA 服务器详细信息以及 Gateway 上配置的 AAA 策略。
  - 安全违规（登录 **>** 安全）：客户端 IP、URL、安全违规（WAF 和机器人）、攻击地理位置、攻击时间戳、交易 ID、WAF 和 NetScaler 安全配置状态。
  - **API** 分析（登录 **>** 安全 **> API** 网关）：有关 API 实例、API 终端节点、总带宽、API 性能信息、总请求、响应时间、错误的信息。能够进一步深入研究每个 API 实例，以了解单个 API 端点和性能。与身份验证成功、失败相关的安全；速率限制、SSL 密码、协议信息和 SSL 错误。

- 安全公告（登录 **>** 基础架构 **>** 实例公告 **>** 安全公告）
  - 版本扫描：此扫描需要 NetScaler 控制台将 NetScaler 实例的版本与可用修复程序的版本和内部版本进行比较。此版本比较有助于 NetScaler 控制台安全公告确定 NetScaler 是否容易受到 CVE 的攻击。本次扫描的基本逻辑是，如果在 NetScaler 发行版上修复了 CVE 并编译了 xx.yy，则所有版本小于 xx.yy 版本的 NetScaler 实例都被视为易受攻击。安全公告目前支持版本扫描。
  - 配置扫描：此扫描需要 NetScaler 控制台将特定于 CVE 扫描的模式与 NetScaler 配置文件进行匹配。如果 NetScaler ns.conf 文件中存在特定的配置模式，则认为该实例容易受到该 CVE 的影响。此扫描通常与版本扫描一起使用。

    今天，安全公告支持配置扫描。
  - 定制扫描：此扫描需要 NetScaler 控制台服务来连接托管的 NetScaler 实例，向其推送脚本并运行脚本。脚本输出有助于 NetScaler 控制台识别 NetScaler 是否容易受到 CVE 的攻击。示例包括特定的 shell 命令输出、特定的 CLI 命令输出、某些日志以及某些目录或文件的存在或内容。如果配置扫描无法解决相同问题，安全公告还会使用自定义扫描来匹配多个配置模式。对于需要自定义扫描的 CVE，脚本会在每次运行预设或按需扫描时运行。有关收集的数据和特定自定义扫描选项的更多信息，请参阅该 CVE 的安全公告文档。

安全性

Citrix Services Security Exhibit 深入描述了应用于 Citrix Cloud Services 的安全控制，包括访问和身份验证、系统开发和维护、安全计划管理、资产管理、加密、运营管理、人力资源安全、物理安全、业务连续性和事件管理。

Citrix Cloud 产品的安全性由加密和密钥管理策略控制。有关 Citrix 如何在整个产品开发生命周期中采用安全的更多详细信息，请参阅安全开发流程白皮书。

NetScaler 控制台服务的数据保留政策

NetScaler 控制台中的统计指标、控制板、报告、警报、事件和日志等数据以及登录详情将在客户订阅该服务期间保留。然后，用户帐户转换为一个 Express 帐户，在该帐户中，用户只能管理两个虚拟服务器。

Express 帐户的容量为 500 MB 或 1 天的分析/报告数据，以帐户先达到的限制为准。如果未使用 Express 帐户，或者客户超过 30 天未登录该帐户，则该帐户和所有相关的客户内容将被自动删除。

有关 Citrix Cloud 服务帐户的数据保留和删除的更多信息，请参阅 Citrix Cloud 服务数据保护概述。

> 注意
>
> NetScaler 控制台中的所有分析数据最多保留 30 天。

第三方服务

NetScaler 控制台服务托管在美国、欧洲、中东和非洲（法兰克福）和亚太及日本（悉尼）地区的 Amazon Web Service (AWS) 数据中心内，具体取决于客户选择的接入点（POP）。

当前，NetScaler 控制台服务使用来自各种第三方技术的服务和 API：

- 用于产品功能的服务：
  - Google Maps、AWS EFS、AWS RDS、AWS Elastic Cache、AWS ALB、AWS Route 53、AWS EKS、AWS Secret Manager、AWS ECR 存储库和 AWS MSK。
- 用于监视和操作 NetScaler 控制台的第三方服务和工具包括：
  - PagerDuty 用于待命轮换
  - 使用 Splunk 进行日志分析
  - 精通日志聚合
  - Slack 用于通信和警报
  - AWS Cloudwatch、SQS
  - S3 作为 AWS 中的存储区域—用于存储核心文件和指标
  - 用于监视的 Prometheus 和 Grafana（在 Honeycomb 部署中）

引用

- 有关我们如何访问所收集数据的更多信息，请参阅 Citrix Services Security Exhibit。
- 有关收集的数据保存多长时间的更多信息，请参阅 Citrix Cloud 服务数据保护概述。
- Citrix Cloud 技术安全概述。
- Citrix Cloud 技术和组织数据安全措施。

快速入门

April 10, 2024

本文档向您介绍如何首次入门和设置 NetScaler 控制台。本文档适用于管理 Citrix 网络设备（NetScaler、NetScaler Gateway、Citrix Secure Web Gateway 等）的网络和应用程序管理员。无论您计划使用 NetScaler 控制台管理哪种设备，都要按照本文档中的步骤进行操作。

在开始入门之前，请务必查看 浏览器要求、代理安装要求和 端口要求。

第 **1** 步：注册 **Citrix Cloud**

要开始使用 NetScaler 控制台，必须先创建 Citrix Cloud 公司帐户或加入贵公司其他人创建的现有帐户。有关如何继续操作的详细流程和说明，请参阅 注册 Citrix Cloud。

第 **2** 步：使用 **Express** 帐户管理 **NetScaler** 控制台

登录 Citrix Cloud 后，执行以下操作：

1. 转至“可用服务”部分。
2. 在“**Application Delivery Management**”图块上，单击“管理”。

   “**Application Delivery Management**”图标移至“我的服务”部分。
3. 选择适合您业务需求的区域。

   > 重要
   >
   > 信息您以后不能更改该区域。

4. 选择适用于您的角色和使用案例。

您可以在后台初始化完成时从浏览器注销，这可能需要一些时间。

> 注意
>
> Citrix 分配一个 Express 帐户来管理 NetScaler 控制台资源。如果您的 NetScaler 控制台 Express 帐户在 45 天内处于非活动状态，则该帐户将被删除。有关更多信息，请参见 使用 Express 帐户管理 NetScaler 控制台。

当您重新登录您的 Citrix Cloud 帐户时，将出现 **NetScaler Con sole GUI** 屏幕。单击“开始”开始首次设置服务。

第 **3** 步：选择 **NetScaler** 部署类型

选择以下适合您的业务需求的部署选项之一：

- 智能部署 -此选项是用于部署新的 NetScaler 实例的自动环境设置。它会自动安装代理以启用 NetScaler 控制台和托管实例之间的通信。

  此选项支持 AWS、Microsoft Azure 和 Google Cloud 环境。通过三个步骤，您可以使用 NetScaler 实例交付存在于云中的应用程序。

- 自定义部署 -此选项是多阶段部署。您可以选择每个环境选项并部署或发现 NetScaler 实例。

为 **AWS** 选择智能部署

此部署选项在 AWS 中创建以下基础设施：

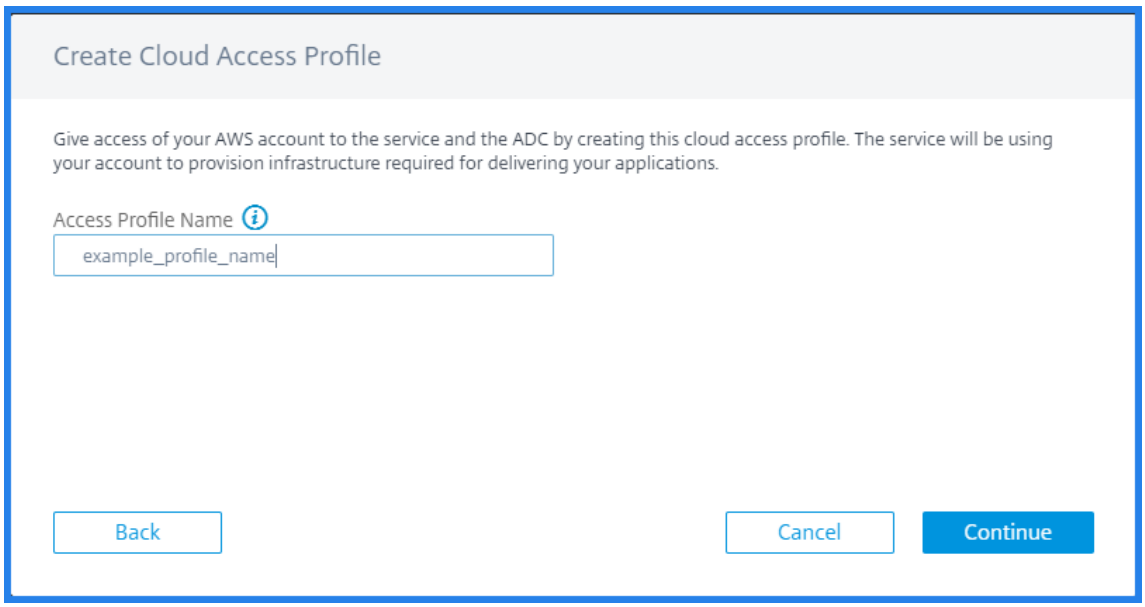
- AWS 中的 CloudFormation 堆栈，用于创建所需的基础设施，包括子网、安全组、NAT 网关等。
- VPC 中的一个代理，用于管理 NetScaler 实例。
- 一个 NetScaler Autoscale 组。您可以稍后在基础结构 **>** 公有云 **> AutoScale** 组页面中自定义该组。

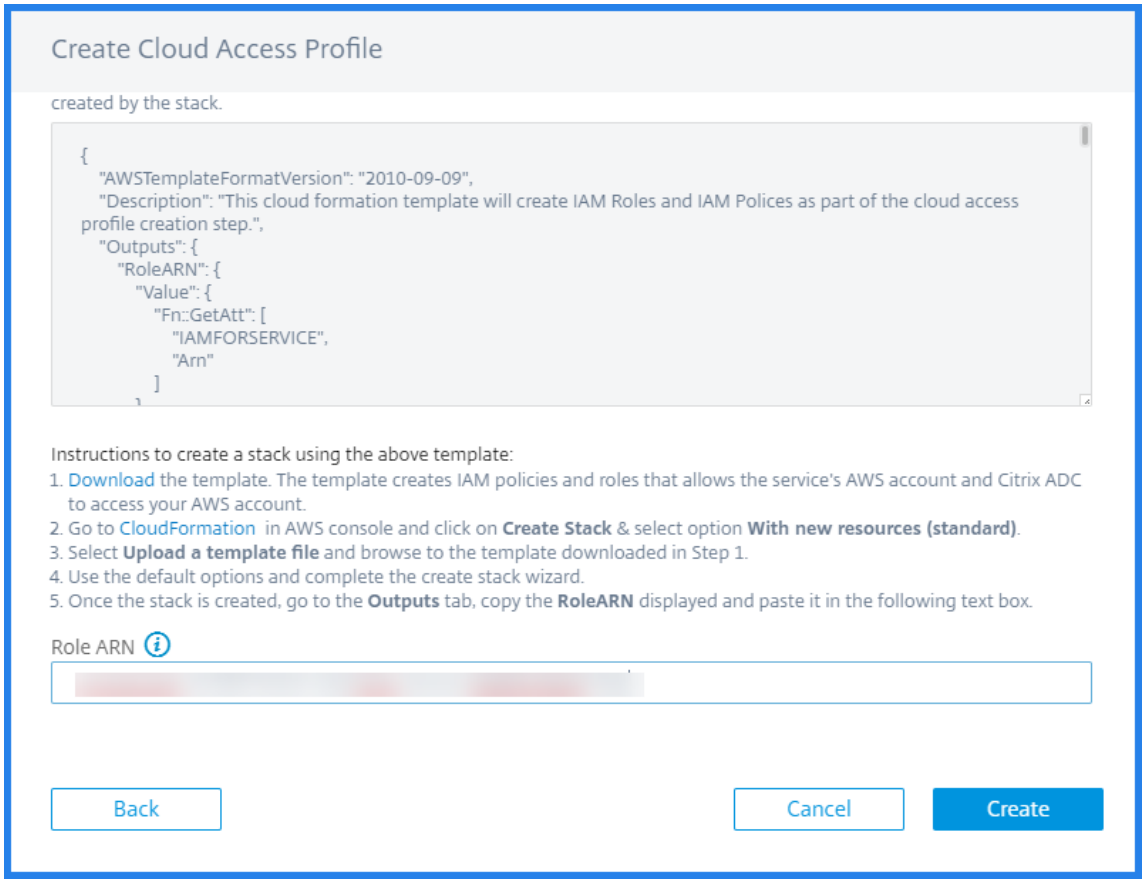
在部署 NetScaler 实例之前，请确保满足以下条件：

1. 您已拥有 AWS 帐户。
2. 您已创建具有所有管理权限的 IAM 用户。

要部署 NetScaler 实例，请执行以下步骤：

1. 在 创建云访问配置文件中，选择 **AWS** 作为部署环境。指定 访问配置文件名称 和 角色 **ARN** 以创建云访问配置文件。





NetScaler 控制台使用云访问配置文件来访问 AWS 帐户。

2. 指定以下详细信息以准备 AWS 环境：

   a) 在 数据中心详情中，选择要部署 NetScaler 实例的 A WS 区域 和 **AWS VPC** 。

   AWS VPC 列出了选定 **AWS** 区域中存在的 VPC。

   b) 在 **NetScaler AutoScale** 组详细信息中，指定以下内容以在 AWS 云中自动扩展 NetScaler 实例：

   - **AutoScale** 组名称 - 用于标识 AutoScale 组的名称。
   - 可用区 -选择要在其中创建 AutoScale 组的区域。

     您可以从列表中选择多个区域。
   - 部署类型 -选择 评估 或 生产 选项。

     如果您想在购买生产许可之前评估 NetScaler 控制台自动缩放解决方案，请选择评估选项。

     > 重要
     >
     > - 评估选项仅支持一个可用区。
     > - 使用评估选项，您只能选择 NetScaler VPX Express。而且，NetScaler 控制台 Autoscale 解决方案最多可以扩展到三个 NetScaler 实例。

- **NetScaler VPX** 产品-选择用于配置 NetScaler 实例的许可证。

  在 AWS 市场中订阅选定的许可证并返回此页面。

  查看并选择用户同意消息。

- 实例类型 -选择所需的实例类型。

c) 单击下一步。

成功验证后，单击“创建”在 AWS 中部署 NetScaler 实例并创建一个 Autoscale 组。

3. 成功部署 NetScaler 后，单击“部署应用程序”。

   在 配置应用程序中，指定必要的详细信息并单击 提交

   有关更多信息，请参阅 为 AutoScale 组配置应用程序。

为 **Microsoft Azure** 选择智能部署

此部署选项在 Azure 中创建以下基础结构：

- 一个 Azure Resource Manager (ARM) 模板，用于创建所需的基础结构，包括子网、安全组、NAT 网关等。
- VPC 中的一个代理，用于管理 NetScaler 实例。
- 一个 NetScaler Autoscale 组。您可以稍后在基础结构 **>** 公有云 **> AutoScale** 组页面中自定义该组。

在部署 NetScaler 实例之前，请确保满足以下条件：

- 您拥有一个支持 Azure Resource Manager 部署模式的 Microsoft Azure 帐户。
- 您在 Microsoft Azure 中有一个资源组。

有关如何创建帐户和其他任务的详细信息，请参阅 Microsoft Azure 文档。

要部署 NetScaler 实例，请执行以下步骤：

1. 在 创建云访问配置文件中，选择 **Microsoft Azure** 作为部署环境。指定 NetScaler 控制台和 NetScaler 云访问配置文件详细信息。

   NetScaler 控制台使用 NetScaler 控制台云访问配置文件访问 Microsoft Azure 帐户。而且，NetScaler 云访问配置文件用于配置 NetScaler VPX 实例。

2. 指定以下详细信息以准备 Azure 环境：

   a) 在 应用程序环境详细信息中，为您的部署指定一个名称。并且，确保选择了正确的云访问配置文件。

   b) 在 数据中心详情中，指定要部署 NetScaler 实例的区域、资源组和虚拟网络详情。

   c) 在 **NetScaler AutoScale** 组详细信息中，指定以下内容：

- 可用性 -选择要在其中创建 AutoScale 组的可用区或集合。根据您选择的云访问配置文件，可用区会显示在列表中。
- 部署类型 -选择 评估 或 生产 选项。

  如果您想在购买生产许可之前评估 NetScaler 控制台自动缩放解决方案，请选择评估选项。

  > 重要
  >
  > - 评估选项仅支持一个可用区或集合。
  > - 使用评估选项，您只能选择 NetScaler VPX Express。而且，NetScaler 控制台 Autoscale 解决方案最多可以扩展到三个 NetScaler 实例。

- 选择 **NetScaler VPX** 产品-选择用于配置 NetScaler 实例的许可证。

  订阅此 Azure 市场许可证并返回页面。

  查看并选择用户同意消息。

- 选择虚拟机大小 -选择所需的虚拟机大小。

d) 单击下一步。

成功验证后，单击“创建”在 Microsoft Azure 中部署 NetScaler 实例并创建一个 Autoscale 组。

3. 成功部署 NetScaler 后，单击“部署应用程序”。

   在 配置应用程序中，指定必要的详细信息并单击 提交

   有关更多信息，请参阅 为 AutoScale 组配置应用程序。

为 **Google Cloud** 选择智能部署

此部署选项在 Google Cloud 中创建以下基础结构：

- 一个 Google Cloud 部署管理器，用于创建所需的基础设施，包括 VPC 网络、子网、Cloud NAT、云路由器网关和防火墙规则。
- VPC 中的一个代理，用于管理 NetScaler 实例。
- 一个 NetScaler Autoscale 组。您可以稍后在基础结构 **>** 公有云 **> AutoScale** 组页面中自定义该组。

在部署 NetScaler 实例之前，请确保您已经拥有一个 Google Cloud 帐户。有关如何创建帐户的更多信息，请参阅 Google Cloud 文档。

要部署 NetScaler 实例，请执行以下步骤：

1. 在 创建云访问配置文件中，选择 **Google Cloud** 作为部署环境。

   指定 云访问配置文件名称 和 服务帐户密钥。

   NetScaler 控制台使用 Cloud Access Profile 来访问 Google Cloud 帐户。

2. 请指定以下详细信息以准备 Google Cloud 环境：

   a) 在 应用程序环境详细信息中，为您的部署指定一个名称。并且，确保选择了正确的云访问配置文件。

   b) 在 数据中心详情中，选择要部署 NetScaler 实例的 **Google** 云区域。

   c) 在 **NetScaler AutoScale** 组详细信息中，指定以下内容以在 Google Cloud 中自动缩放 NetScaler 实例：

   - **VPC** 网络的子网 **CIDR** -指定为管理、客户端和服务器流量创建的 VPC 网络。但是，您可以为服务器选择现有网络。
   - 区域 -选择要在其中创建 AutoScale 组的区域。

     您可以从列表中选择多个区域。
   - 部署类型 -选择 评估 或 生产 选项。

     如果您想在购买生产许可之前评估 NetScaler 控制台自动缩放解决方案，请选择评估选项。

     > 重要
     >
     > - 评估选项仅支持一个可用区。
     > - 使用评估选项，您只能选择 NetScaler VPX Express。而且，NetScaler 控制台 Autoscale 解决方案最多可以扩展到三个 NetScaler 实例。

   - **NetScaler VPX** 产品-选择用于配置 NetScaler 实例的许可证。
   - 机器类型 -选择所需的实例类型。

   d) 单击下一步。

   成功验证后，单击“创建”，在 Google Cloud 中部署 NetScaler 实例并创建一个 Autoscale 组。

3. 成功部署 NetScaler 后，单击“部署应用程序”。

   在 配置应用程序中，指定必要的详细信息并单击 提交

   有关更多信息，请参阅 为 AutoScale 组配置应用程序。

选择自定义部署

此选项提供多阶段部署。选择此选项可发现来自各种环境的 NetScaler 实例。使用此选项，您还可以通过指定自定义环境选项来部署新实例。

执行以下步骤来部署或发现 NetScaler 实例：

1. 选择以下任一环境：

   - **AWS**
   - **Microsoft Azure**

- **Google** 云端平台
- 本地

2. 安装代理以启用 NetScaler 控制台与数据中心或云中的托管实例之间的通信。

   “选 择代理类型”步骤根据所选环境的不同而改变代理安装选项。

   - 本地 -如果您选择 本地，则可以在以下虚拟机管理程序上安装代理：
     - Citrix Hypervisor
     - VMware ESXi
     - Microsoft Hyper-V
     - Linux KVM 服务器
   - 公有云 -如果您选择 **AWS**、**Microsoft Azure** 或 **Google Cloud Platform**，则可以在所选云上外部安装代理。

     以下是 AWS 环境的示例图像。
   - 作为微服务 -将代理部署为 Kubernetes 应用程序。
   - 内置代理 -发现 NetScaler 12.0 版或更高版本中可用的内置代理。

3. 单击 **Next**（下一步）

   安装代理的步骤因每个选项而异。以下链接将引导您进入安装代理的具体步骤：

   - 虚拟机管理程序
   - 外部代理
   - 作为微服务
   - 内置代理

在 **Hypervisor** 上安装代理

执行以下步骤，在虚拟机管理程序上设置代理：

1. 选择虚拟机管理程序，然后单击 下载映像，将代理映像下载到本地系统。

   生成服务 URL 和激活码并显示在 GUI 上。

2. 复制服务 URL 和激活码。
3. 在虚拟机管理程序上安装代理时，请指定复制的服务 URL 和激活码。

   代理使用服务 URL 查找服务，并使用激活代码向服务注册。有关在本地虚拟机管理程序上安装代理的详细说明，请参阅本地 安装代理。

4. 成功安装代理后，返回“设置代理”页面，然后单击 注册代理。

下一步：添加实例。

> 注意
>
> 如果您不想在初始设置期间添加代理，请单击“跳过”以检查 NetScaler 控制台提供的功能。您可以稍后添加代理和实例。要稍后添加代理，请导航到“设置”>“设置客户端”。有关以后如何添加实例的说明，请参阅 添加实例。

在公有云上安装代理

您不必从设置代理页面下载代理映像。客户端映像在相应的云市场上可用。

1. 复制并保存要在代理安装过程中使用的服务 URL 和激活码。

   如果您想要新的激活码，请单击 创建新的激活码，然后复制并保存要在代理安装期间使用的代码。

   - 有关在微软 Azure 云上安装代理的详细说明，请参阅在 Microsoft Azure 云上安装代理。
   - 有关在 AWS 上安装代理的详细说明，请参阅在 A WS 上安装代理。
   - 有关在 Google Cloud 上安装代理的详细说明，请参阅在 GCP 上安装代理。

2. 成功安装代理后，返回“设置代理”页面，然后单击 注册代理。

下一步：添加实例。

将代理安装为微服务

您可以将代理作为微服务部署在 Kubernetes 群集中，以便在 NetScaler 控制台中查看服务图。

有关开始使用服务图的更多信息，请参阅 设置服务图。

1. 指定以下参数：

   a) 应用程序 **ID** —一个字符串 ID，用于为 Kubernetes 群集中的代理定义服务并将此代理与同一群集中的其他代理区分开来。

   b) 代理密码—指定一个密码，让 CPX 使用此密码通过代理将 CPX 载入 NetScaler 控制台。

   c) 确认密码—指定相同的密码进行确认。

   d) 单击 **Submit**（提交）。

2. 单击“提交”后，您可以下载 YAML 或 Helm 图表。
3. 单击关闭。

   有关更多信息，请参见 在 Kubernetes 群集中安装代理。

使用内置代理

您的环境中的 NetScaler 实例包含内置代理。您可以启动内置代理并使用它在实例和 NetScaler 控制台之间建立通信。

1. 复制生成的 服务 **URL** 和 激活码。保存它们以便在 NetScaler 实例上启动内置代理时使用。

   有关在 NetScaler 实例上启动内置代理的详细说明，请参阅在 Citrix ADC 实例上启动内置代理。

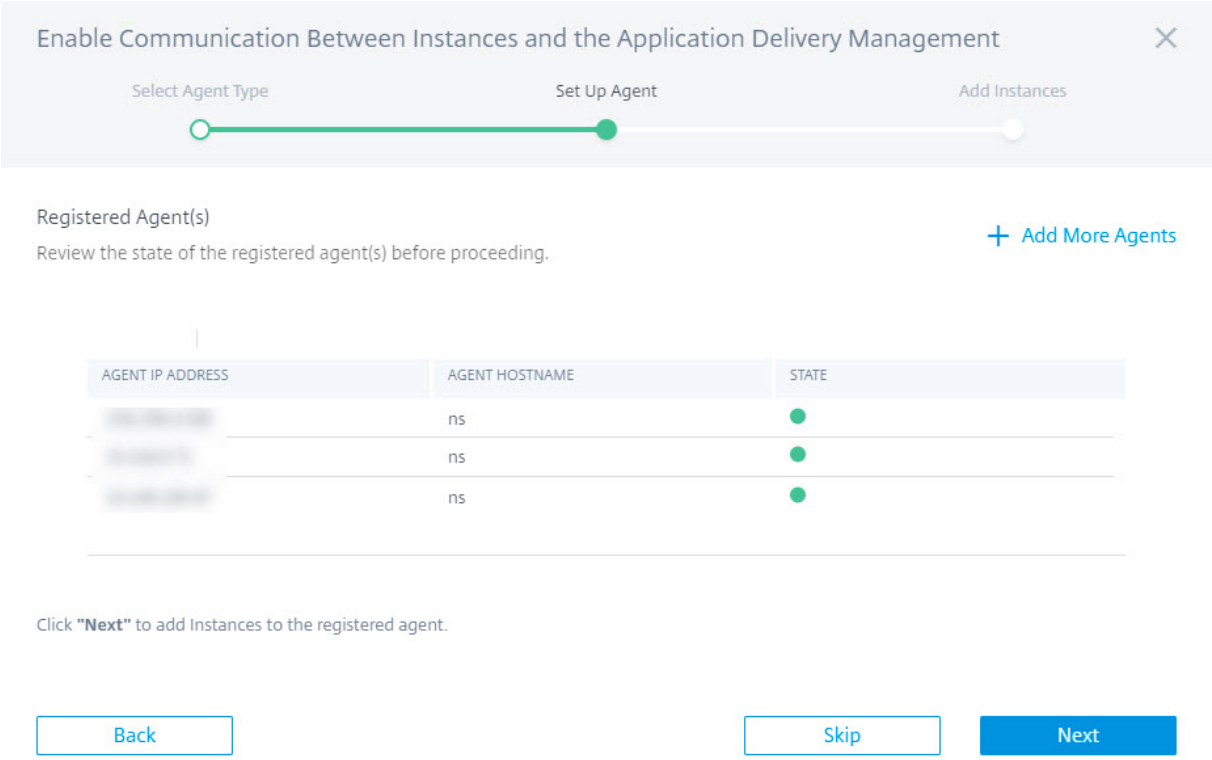
2. 启动内置代理后，返回 设置代理 页面，然后单击 注册实例。

下一步：添加实例。

添加实例

实例是您要从 NetScaler 控制台发现、管理和监视的网络设备或虚拟设备。要管理和监视这些实例，您必须将实例添加到服务中。

成功安装和注册代理后，代理将显示在“设置代理”页面上。当代理状态处于运行状态，由旁边的绿色圆点表示时，单击 **Next**（下一步）开始向服务添加实例。



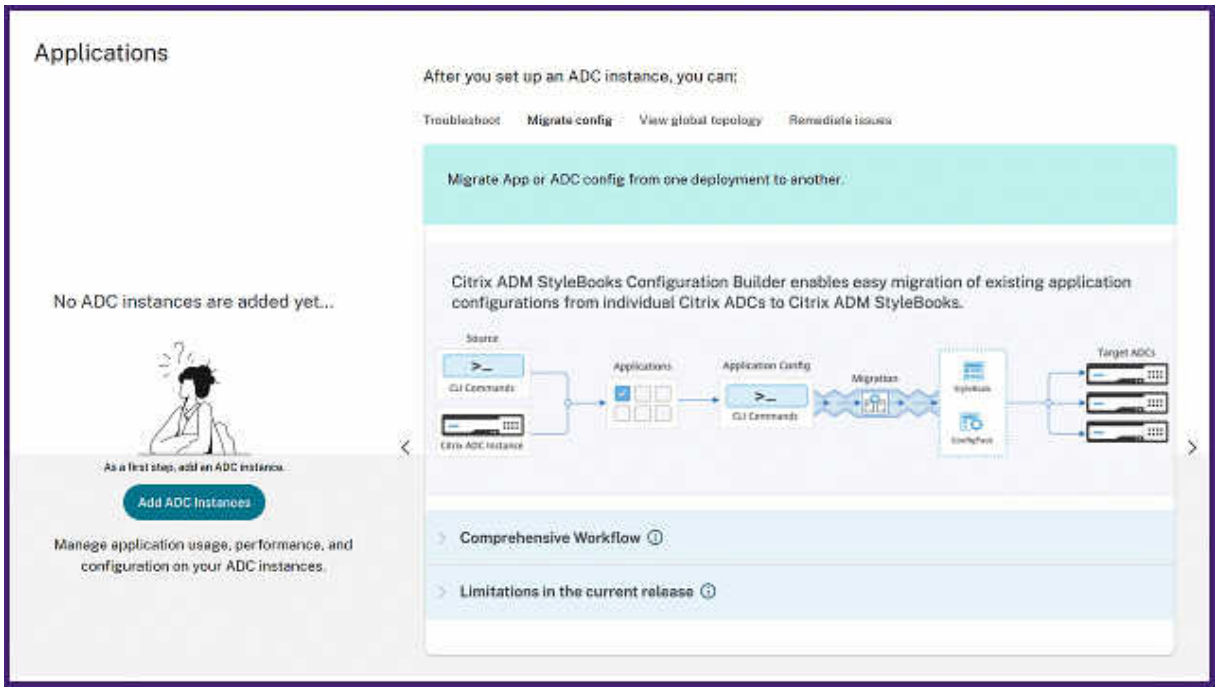
1. 在“添加实例”页面中，查看连接到注册代理的 NetScaler 实例。确保实例处于 **Up** 状态，然后单击 **Next**。
2. 单击 完 成以完成初始设置并开始管理您的部署。

> 注意
>
> 如果您不想在初始设置期间添加实例，可以单击“完成”完成设置，稍后再添加实例。有关稍后如何向 NetScaler 控制台添加实例的说明，请参见添加实例。

使用 **NetScaler** 控制台 **GUI** 控制面板加载 **NetScaler** 实例

如果您在首次设置 NetScaler 控制台时跳过了入 门工作流程 中的 NetScaler 实例的加载，则可以从 NetScaler 控制台 GUI 控制面板加载实例。如果尚未添加 NetScaler 实例，GUI 会提示您添加实例。

当您单击左侧导航栏上的任何模块时，右侧会显示该模块的功能和优点的表格预览。这些功能和优势可帮助您使用 NetScaler 控制台更好地管理 NetScaler 实例。

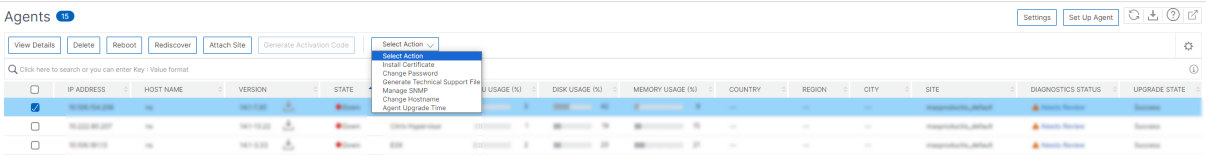


单击“添加 **NetScaler** 实例”以载入实例。“入门”工作流程重新启动。按照本文档中给 出的步骤 3：选择一种 NetScaler 部署 类型及以后的步骤来载入实例。

如果 NetScaler 实例已经载入，则在您登录到 NetScaler 控制台后，您只能看到左侧导航栏的 NetScaler 控制台登录页面。

代理行动

设置 NetScaler 控制台后，您可以对代理应用各种操作。导航到 基础结构 **>** 实例 **>** 代理。



在“选择操作”下，您可以使用以下功能：

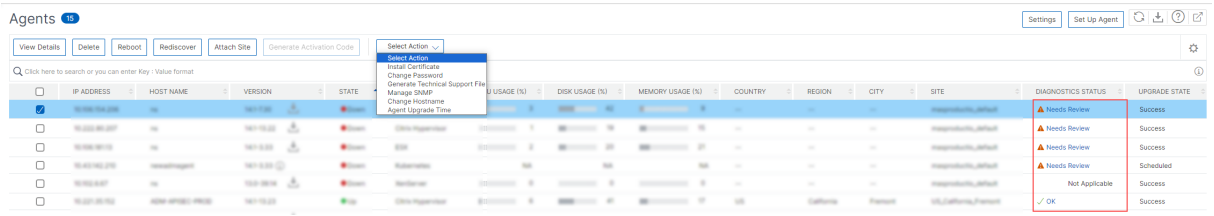
- 安装新证书：如果您需要不同的代理证书来满足您的安全要求，则可以添加一个。
- 更改代理密码：为确保基础结构的安全，请更改代理的默认密码。
- 生成技术支持文件：为所选代理生成技术支持文件。您可以下载此文件并将其发送给 Citrix 技术支持部门进行调查和故障排除。

查看代理诊断并接收端点验证警报

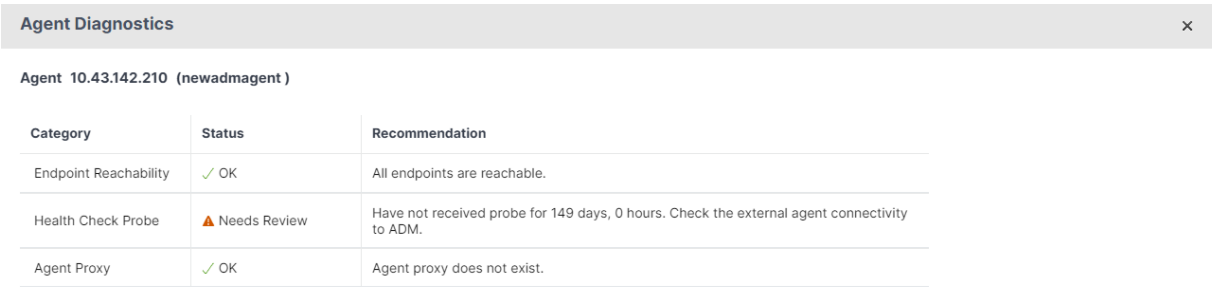
NetScaler 控制台定期（每隔一小时）对代理执行诊断检查并提供以下信息：

- 端点可访问性 -检查所有端点是否均可访问。该代理使用各种端点在 NetScaler 控制台和 NetScaler 实例之间进行通信。有关更多信息，请参阅 软件要求。
- 运行状况检查探测器 -提供最新运行状况检查的时间戳。
- 代理代理 -检查代理代理是否存在。

如果代理端点的可访问性状态发生变化（从正常更改为需要审核），则超级管理员会收到一封包含问题详细信息的电子邮件通知。导航到 基础结构 **>** 实例 **>** 代理，查看新添加的“诊断状态”选项，该选项提供了“需要审查”或“确定”等状态。



单击查看代理的诊断信息。

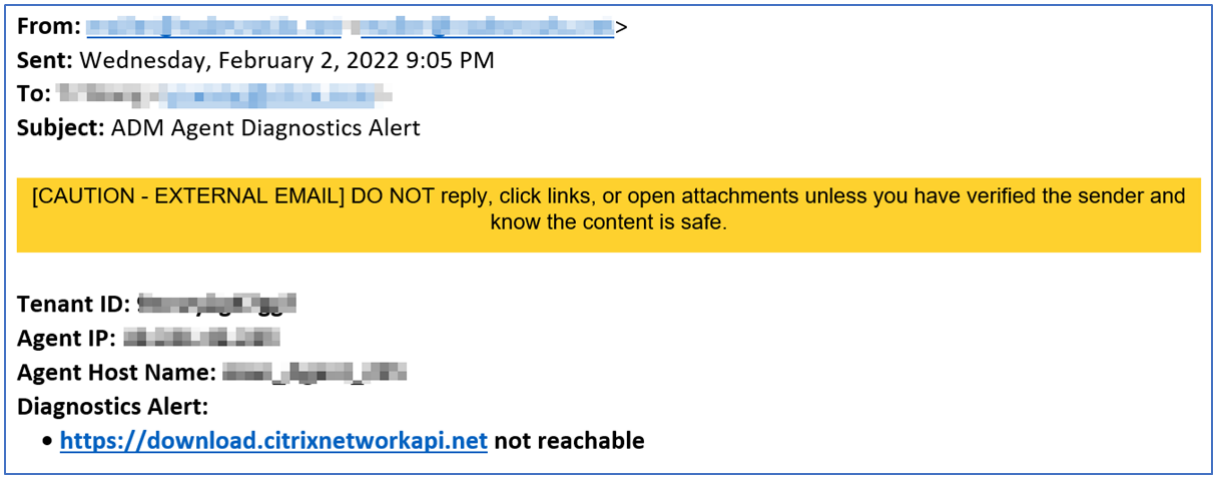


- **Category**（类别）。提供问题类别。
- 状态。提供问题状态，例如“需要审查”或“正常”。
- 建议。提供解决问题所需的建议。

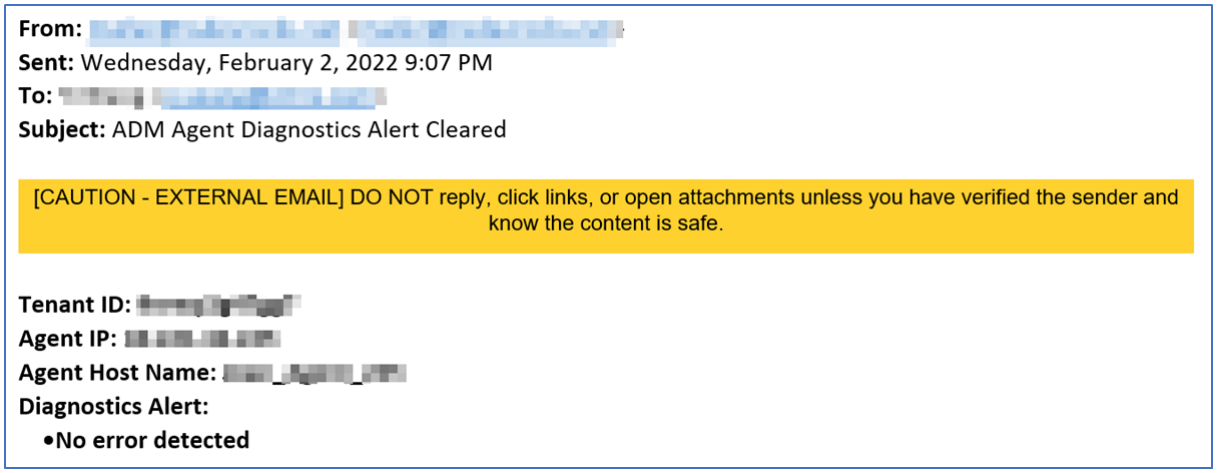
在您进行故障排除并且端点可访问性状态从“需要审查”更改为“正常”后，超级管理员会收到一封电子邮件通知，告知问题已解决。

电子邮件通知

以下示例是端点可访问性状态从正常更改为需要审查之后的电子邮件通知：



以下示例是端点可访问性状态从“需要审查”更改为“正常”之后的电子邮件通知：



配置内置代理来管理实例

January 29, 2024

在运行版本 12.1.48.13 及更高版本的 NetScaler MPX、VPX、网关实例以及运行 13.0 61.x 及更高版本和 12.1 58.x 及更高版本的 NetScaler SDX 实例上均提供内置代理。您可以在 NetScaler 实例上启动此代理，而不必在数据中心或公有云中安装专用代理。内置代理支持实例与 NetScaler 控制台之间的通信。

> 注意：
>
> 内置代理仅适用于以下 NetScaler 实例类型：
>
> - NetScaler MPX
> - NetScaler VPX
> - NetScaler SDX
> - NetScaler Gateway

内置代理非常适合较小的 NetScaler 独立部署或 HA 对部署。如果您有多个 NetScaler 实例，请使用专用代理进行部署。该代理可确保您拥有比内置代理更好的数据聚合功能。有关更多信息，请参阅 在本地安装代理。

NetScaler 控制台支持使用内置代理管理和监视 NetScaler 实例。但是，内置代理不支持以下功能：

- “应用程序”控制板
- Web Insight
- SSL Insight
- HDX Insight
- Gateway Insight
- Security Insight
- 高级分析
- 池许可

您可以从内置代理过渡到外部代理。有关更多信息，请参阅 从内置代理过渡到外部代理。

必备条件

在 NetScaler 实例上配置内置代理之前，请确保以下操作：

- NetScaler（MPX、VPX 或网关）实例正在版本 `12.1.48.13` 或更高版本上运行。SDX 实例正在运行版本 `13.0.61.x` 及更高版本。
- 将在 NetScaler 实例上添加 DNS 名称服务器。

  有关更多信息，请参阅 添加域名服务器。
- 您有一个 Citrix Cloud 帐户。有关详细信息，请参阅注册 Citrix Cloud。

> 注意：
>
> 有关端口和其他系统要求的所有信息，请参阅 系统要求。

配置内置代理

执行以下任务以配置 NetScaler 内置代理：

1. 按照“入门”中的说明选择内置代理选项。
2. 复制 服务 **URL** 和 激活码。

   代理使用服务 URL 查找服务，并使用激活代码向服务注册。如果您是 MPX 或网关客户，请跳过步骤 7。
3. 使用 SSH 客户端启动内置代理。网关用户必须跳过此步骤。

   a) 登录到您的 NetScaler 实例。有关更多信息，请参阅 访问 NetScaler。

   b) 导航到目 `/var/mastools/scripts` 录并键入以下命令：

   在 **SDX** 实例上

	使用 NetScaler 帐户注册	在没有 NetScaler 配置文件的情况下注册
–	–	–
前提条件	在注册之前，创建一个 NetScaler 配置文件。有关更多信息，请参阅如何创建 **NetScaler** 配置文件。
运行此命令	**./mastools_init.sh <device-profile-name> <service-url> <activation-code> -sdx -profile**	**./mastools_init.sh <user_name> <service-url> <activation-code> -sdx**
用户凭据	在 <device_profile_name> 中输入 nsroot。或者，您可以使用与 nsroot 具有相同访问权限的用户名。	在 <user_name> 中输入 nsroot。或者，您可以使用与 nsroot 具有相同访问权限的用户名。

   > 注意：
   >
   > NetScaler 控制台会发现在该软件开发工具包上运行的所有 VPX 实例，您无需单独注册 VPX 实例。

   在未在 **SDX** 设备上运行的 **VPX** 实例以及 **MPX** 和网关实例上：

   如果 NetScaler 镜像版本低于 13.0 61.x 或 12.1 57.x，则必须通过键入 `cat /var/mastools/version.txt` 命令来检查 `mastools` 版本。如果输出是 `0.0-0.0`，这是第一次。

   根据软件版本键入以下命令之一。

   > 注意：
   >
   > 在注册 NetScaler 配置文件之前，必须创建该配置文件。有关更多信息，请参阅 如何创建 NetScaler 配置文件。

NetScaler 镜像版本	Is mastools_version 0.0-0.0?	用配置文件注册的命令	没有配置文件的注册命令
低于 13.0 61.xx 和 12.1 57.xx	是	./mastools_init.sh <device_profile_name> <service_url> "MAS;<activation_code>"-profile	./mastools_init.sh <user_name><pwd> <service_url> "MAS;<activation_code>"
低于 13.0 61.xx 和 12.1 57.xx	否	./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile	./mastools_init.sh <user_name><pwd> <service_url> <activation_code>
高于 13.0 61.x 和 12.1 57.xx	不适用	./mastools_init.sh <device_profile_name> <service_url> <activation_code> -profile	./mastools_init.sh <user_name><pwd> <service_url> <activation_code>

> 注意：
>
> - 在 <device_profile_name> 或 <user_name> 中，输入 nsroot。或者，您可以使用与 nsroot 具有相同访问权限的用户名。
> - 在 HA 对中，在主节点上完成注册。如果您在辅助节点上运行注册命令，则会出现以下消息：请在主节点上运行注册命令。

4. 返回 NetScaler 控制台页面，然后单击“注册实例”。
5. 在 添加实例中，查看您启动内置代理的实例。确保实例处于 **Up** 状态，然后单击 **Next**。
6. 单击 **Done**（完成）。

成功配置内置代理后，您可以访问 NetScaler 控制台功能，例如：

- 虚拟服务器和分析—向您的虚拟服务器申请许可证以管理 NetScaler 实例。有关更多信息，请参阅 管理订阅。
- 应用程序控制板 -以整体方式查看所有应用程序。有关更多信息，请参阅 应用程序管理和控制板。

- 基础设施分析 -此功能可帮助您可视化导致或可能导致实例问题的因素。有关更多信息，请参阅 基础结构分析

> 注意
>
> 您也可以通过导航到 基础结构 > 实例 > 代理 > 生成激活码 页面来配置内置代理。将 URL 和激活码复制并粘贴到 NetScaler 实例，然后发现该实例。

启动内置代理后，导航到 基础结构 > 实例 > **NetScaler**。此页显示有关使用内置代理发现的托管实例的详细信息。

故障排除

如果注册失败或者注册成功但内置代理未出现在 NetScaler 控制台 GUI 中，您可以检查日志。

- 如果注册失败，请检查登录 `/var/mastools/logs/mastools_reg.py.log`
- 如果注册成功，但内置代理未出现在 NetScaler 控制台 GUI 中，请检查：
  - `/var/mastools/logs/mastools_upgrade.log` 中的 **mastools_Upgrade** 日志
  - `/var/log/mastoolsd.log` 中的二进制日志。

在本地安装 **NetScaler** 代理

January 29, 2024

该代理充当 NetScaler 控制台和在数据中心发现的实例之间的中介。

在开始安装代理之前，请确保您拥有 Hypervisor 必须为每个代理提供的所需虚拟计算资源。有关更多信息，请参阅 代理安装要求 和 池化许可的轻量代理。

> 注意
>
> 有关端口和其他要求的所有信息，请参阅 支持的端口。

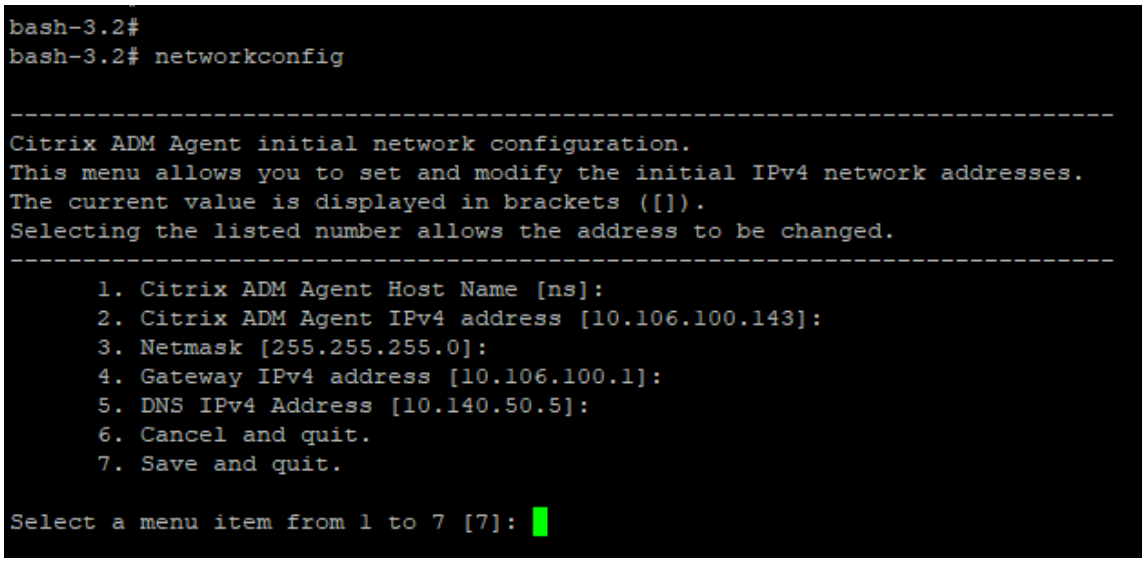
要安装 **NetScaler** 代理，请执行以下操作：

1. 按照 入门中的说明下载代理映像。
2. 将代理映像文件导入虚拟机管理程序。
3. 在 控制台 选项卡中，配置初始网络配置选项，如以下示例所示：

> 注
>
> 意确保将 DNS 配置为允许互联网访问您的 NetScaler 代理。

4. 完成初始网络配置后，保存配置设置。出现提示时，使用默认 (`nsrecover`/`nsroot`) 凭据登录。

   如果要更改代理上已配置的网络设置，请键入 `networkconfig` 命令并按照 CLI 中的提示进行操作。

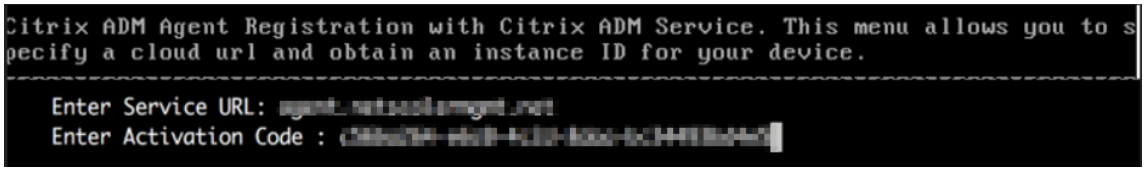


5. 如果没有提示输入服务 URL，请在 NetScaler 代理中导航到 /mps，然后运行以下任一脚本：

```
1 deployment_type.py
```

```
1 register_agent_cloud.py
```

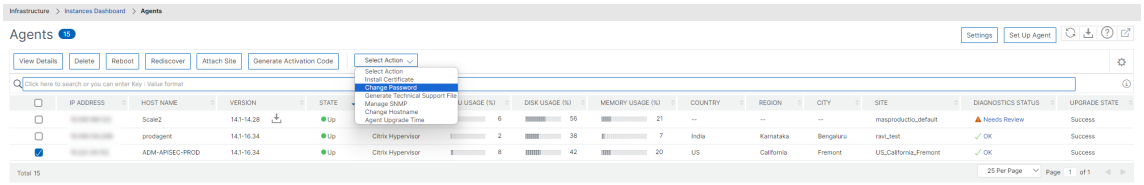
6. 输入您在下载代理镜像时保存的 服务 **URL** 和 激活码。代理使用服务 URL 查找服务，并使用激活代码向服务注册。



7. 代理注册成功后，代理程序将重新启动以完成安装过程。

代理重新启动后，访问 NetScaler 控制台 GUI 并导航 到基础架构 **>** 实例 代理以验证代理的状态。配置代理后，必须更改密码。

1. 导航到 基础结构 **>** 实例 **>** 代理
2. 选择代理，然后从“选择操作”列表中单击“更改密码”。



3. 输入当前密码 (`nsroot`)，然后指定新密码，然后单击“确定”更改密码。

   密码必须：

   - 长度至少为六个字符
   - 至少包含一个特殊字符
   - 至少包含一个大写字符
   - 至少包含一个小写字符
   - 至少包含一个数字字符

在 **Microsoft Azure** 云上安装 **NetScaler** 代理

January 29, 2024

该代理充当 NetScaler 控制台与企业数据中心或云端托管实例之间的中介。

要在 Microsoft Azure 云上安装 NetScaler 代理，您必须在虚拟网络中创建该代理的实例。从 Azure Marketplace 获取 NetScaler 代理镜像，然后使用 Azure Resource Manager 门户创建代理。

在开始创建 NetScaler 代理实例之前，请确保已使用该实例所在的所需子网创建了一个虚拟网络。可以在 VM 置备期间创建虚拟网络，但无法灵活地创建不同的子网。有关创建虚拟网络的信息，请参阅 http://azure.microsoft.com/en-us/documentation/articles/create-virtual-network。

配置 DNS 服务器和 VPN 连接，允许虚拟机访问互联网资源。

必备条件

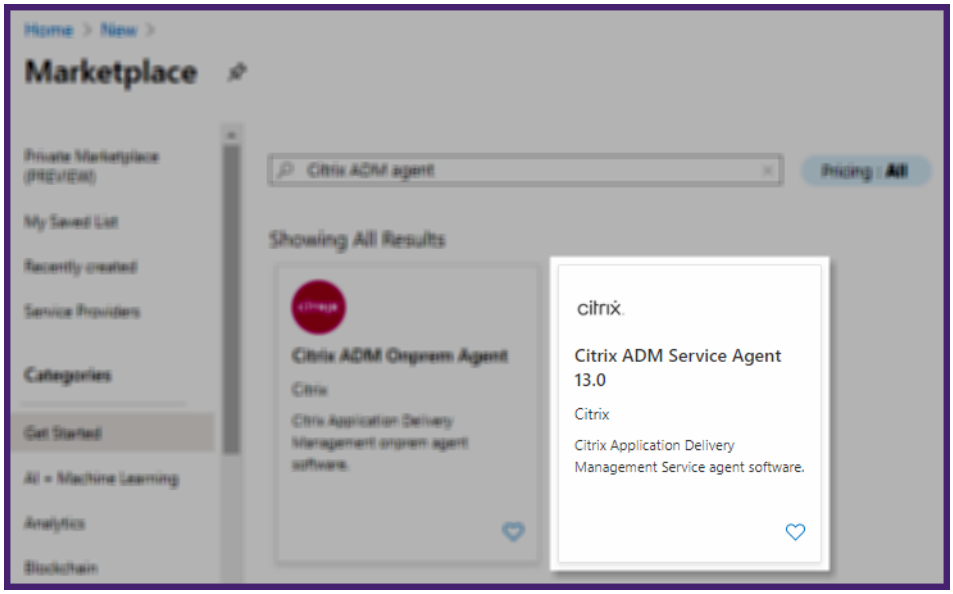
请确保您具备以下项：

- Microsoft Azure 用户帐户
- Microsoft Azure Resource Manager 的访问权限

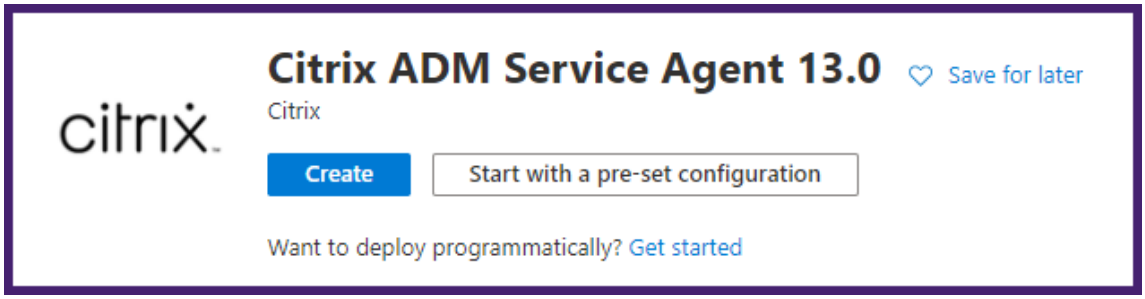
> 注意
>
> - 我们建议您在配置 NetScaler 代理虚拟机之前创建资源组、网络安全组、虚拟网络和其他实体，以便网络信息在配置期间可用。
> - 要让 NetScaler 代理与 NetScaler 控制台和 NetScaler 实例通信，请确保推荐的端口处于打开状态。有关 NetScaler 代理的端口要求的完整详细信息，请参见端口。

要在 **Microsoft Azure** 云上安装 **NetScaler** 代理，请执行以下操作：

1. 使用您的 Microsoft Azure 凭据登录 Azure 门户 (https://portal.azure.com)。
2. 单击 **+** 创建资源。
3. `NetScaler agent`在搜索栏 中键入并选择 **NetScaler** 代理。



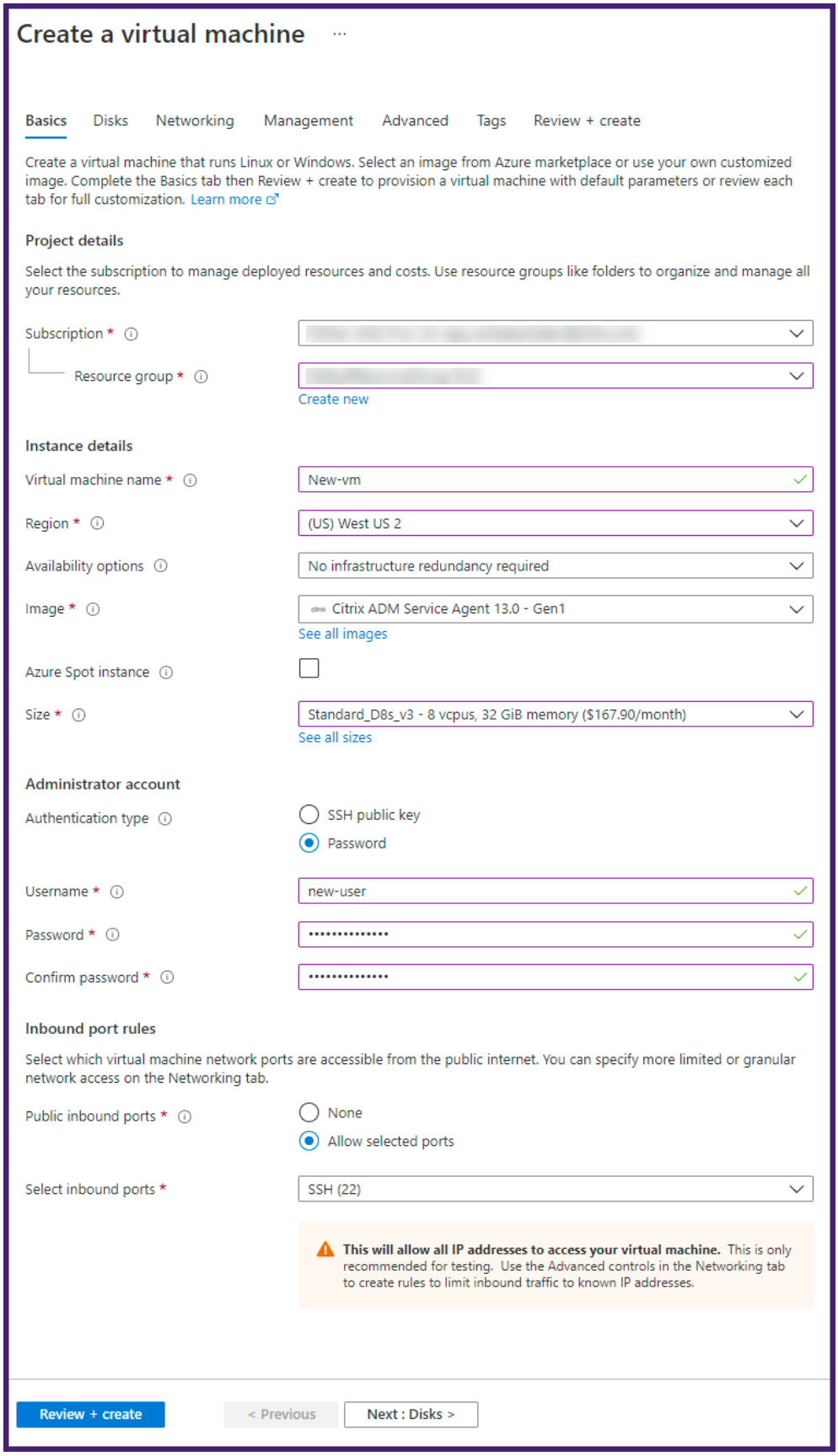
4. 单击创建。



5. 在 **Create virtual machine**（创建虚拟机）窗格中，在各个部分中指定所需的值以创建虚拟机。

   基础知识：

在此选项卡中，指定 项目详细信息、实例详细信息和 管理员帐户。



- 资源组 - 从下拉列表中选择您创建的资源组。

  > 注意
  >
  > 此时您可以创建资源组，但我们建议您在 Azure Resource Manager 中从“资源组”中创建资源组，然后从下拉列表中选择该组。

- 虚拟机名称 -指定 NetScaler 代理实例的名称。
- 区域 -选择要部署代理的区域。
- 可用性选项—从列表中选择可用性集。
- 图像 -此字段显示已选择的座席映像。如果要更改为其他代理映像，请从列表中选择所需的映像。
- 大小 - 指定用于部署 NetScaler 代理的虚拟磁盘的类型和大小。

  从列表中选择支持的虚拟磁盘类型（**HDD** 或 **SSD**）。

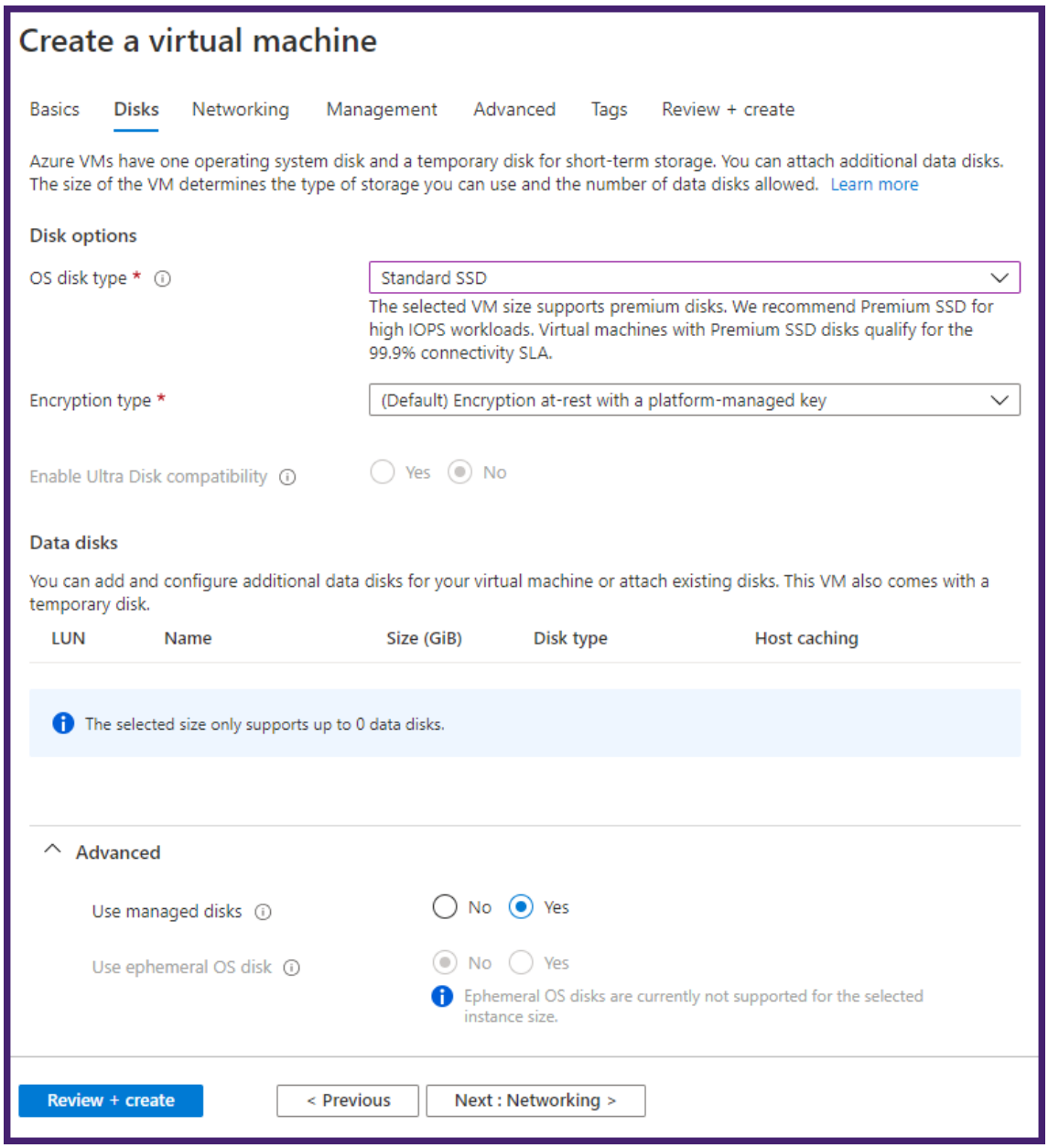
  有关支持的虚拟磁盘大小的更多信息，请参阅 代理安装要求 和 池化许可的轻量代理。

- 身份验证类型—选择密码。
- 用户名和密码—指定用户名和密码以访问您创建的资源组中的资源。

  > 重要
  >
  > 我们建议您为代理指定自己的用户名和密码。请勿使用 `nsrecover` 或 `nsroot` 作为用户名，因为它们是为代理用户保留的。

磁盘：

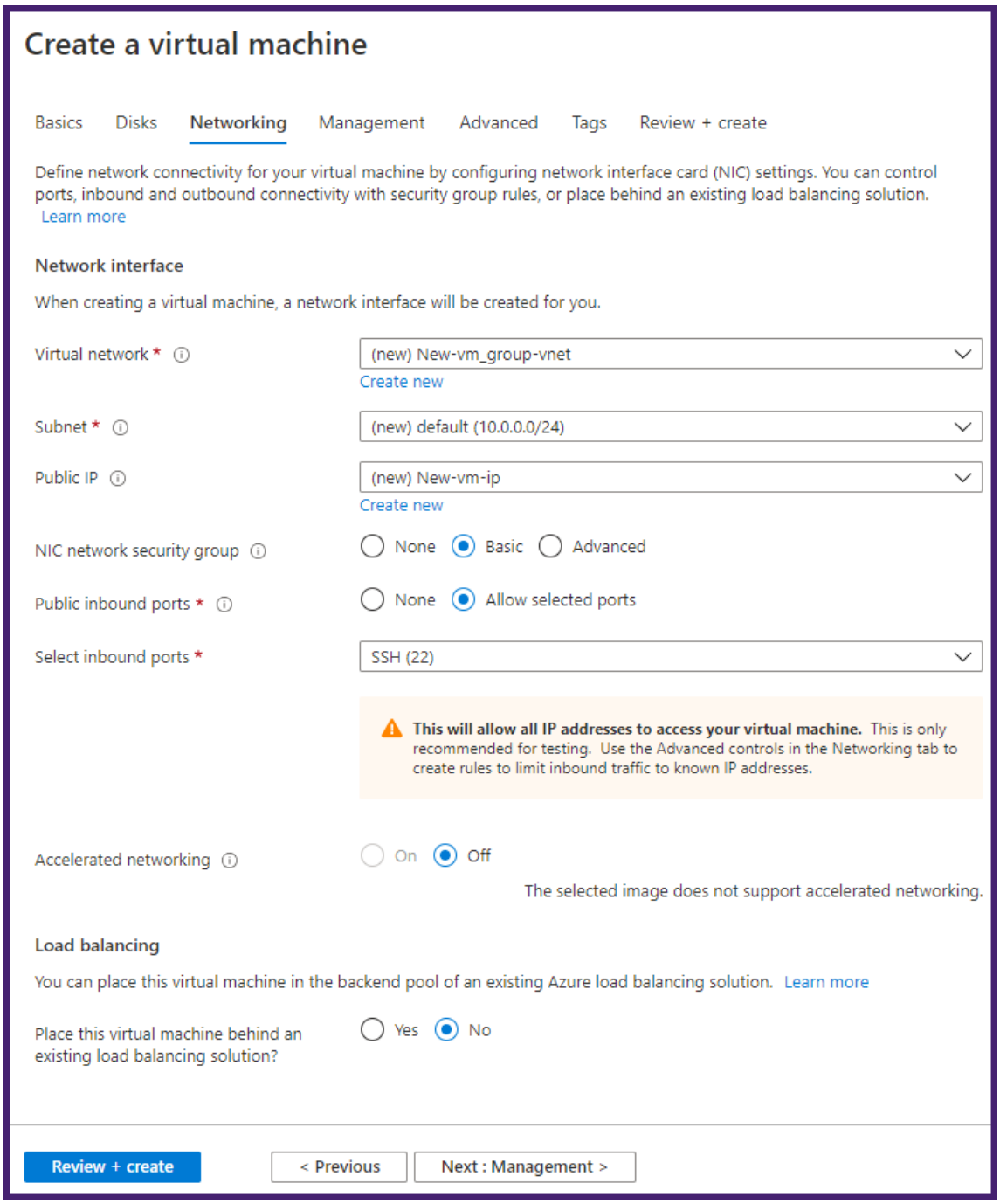
在此选项卡中，指定 磁盘选项 和 数据磁盘。



- 操作系统磁盘类型 -选择虚拟磁盘类型（HDD 或 SSD）。

网络连接**:**

指定所需的网络详细信息：

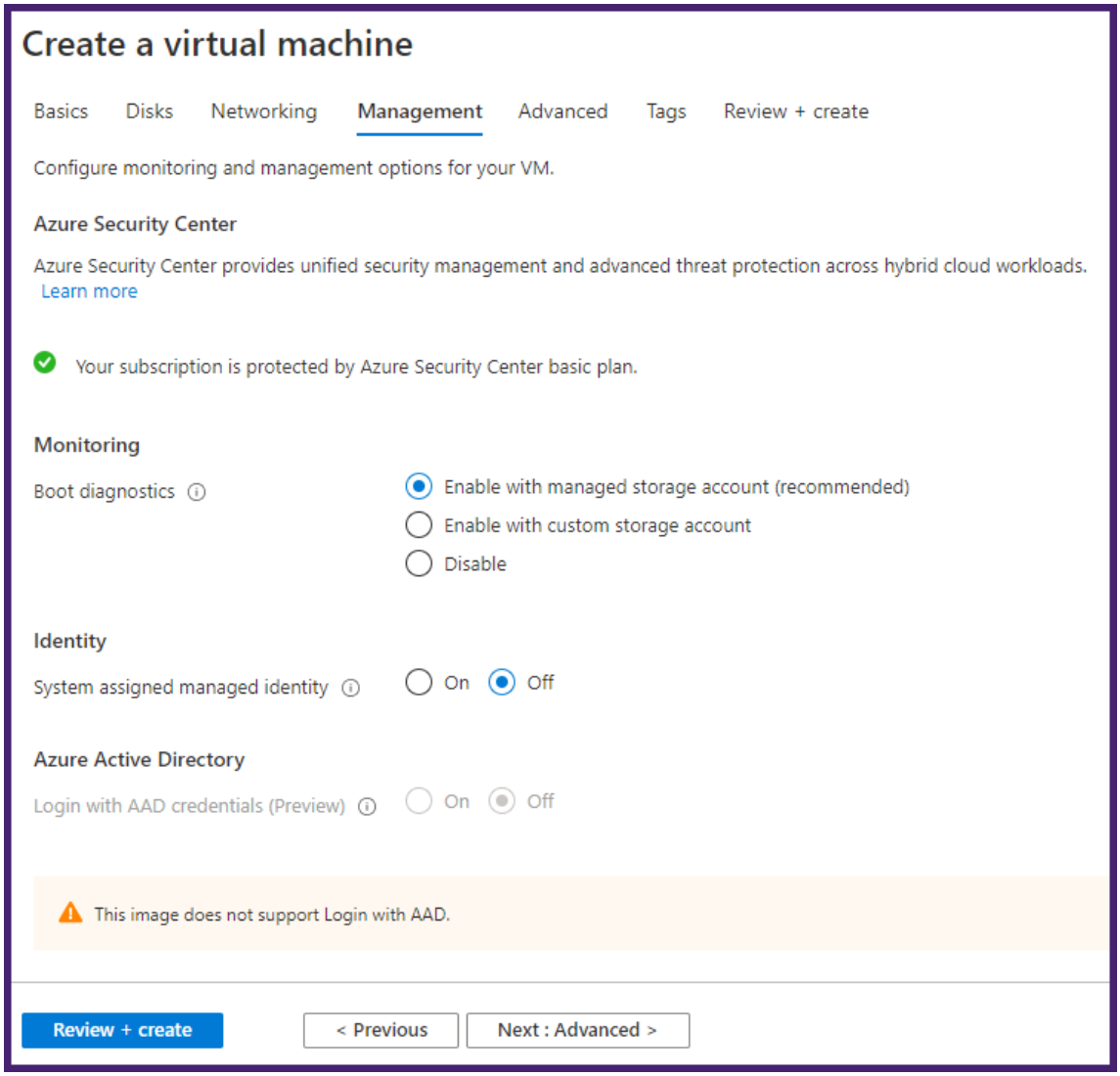


- 虚拟网络—选择虚拟网络。
- 子网 -设置子网地址。
- 公有 **IP** 地址 -可选，选择 IP 地址。
- 网络安全组 -可选，选择您创建的安全组。
- 选择入站端口 -如果允许公用入站端口，请确保在安全组中配置了入站和出站规则。然后，从列表中选择入站端口。有关详细信息，请参阅先决条件

> 注意
>
> 确保代理可以访问互联网。

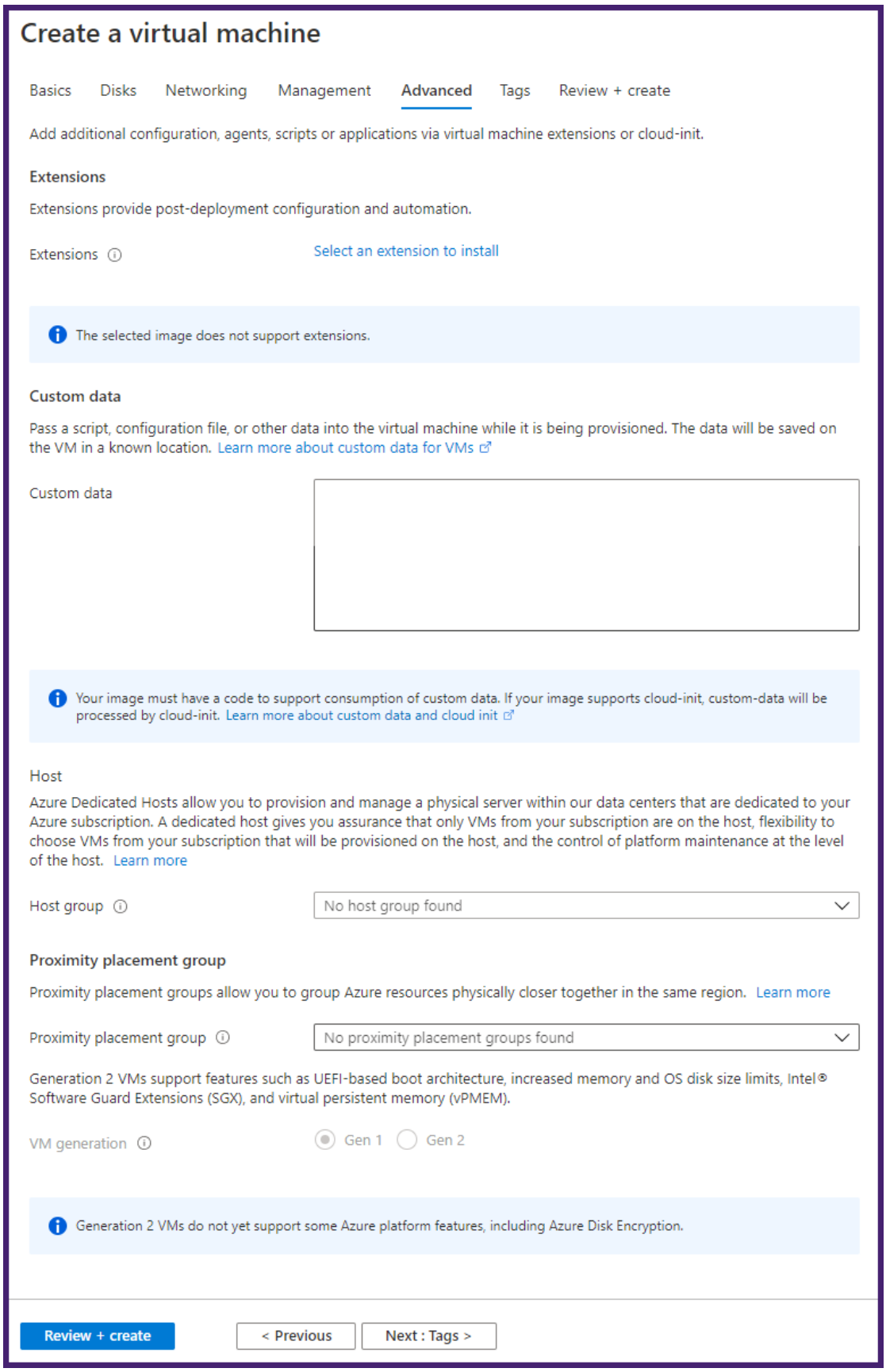
管理层：

指定 **Azure** 安全中心、监视和 身份。



高级：

可选，指定 扩展程序、自定义数据和 邻近置放组。

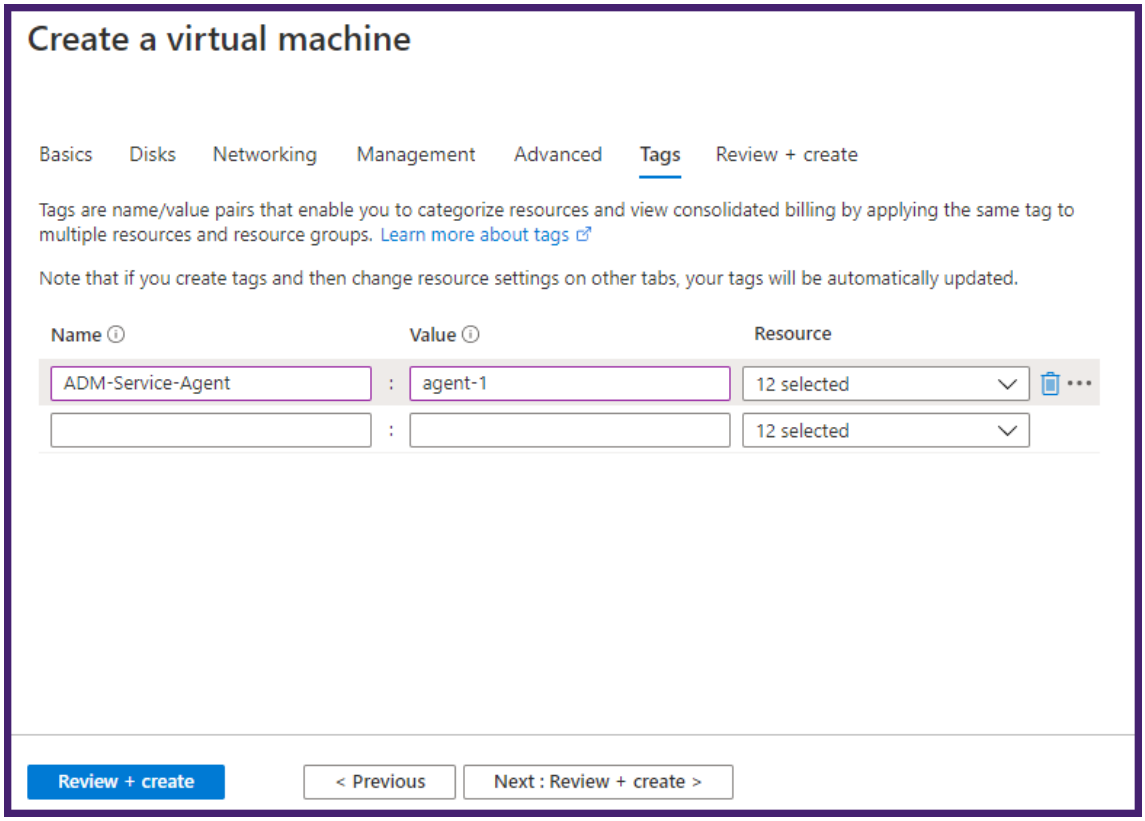


> 注意
>
> 在 定制数据中，按照入门中的说明指定您从 NetScaler 控制台的“设置代理”页面复制的 服务 **URL** 和激活码。按以下格式输入详细信息：
>
> ```
> registeragent -serviceurl <apigatewayurl> -activationcode <
>     activationcodevalue>
> ```
>
> 代理使用此信息在启动期间自动注册到 NetScaler 控制台。

如果指定此自动注册脚本，请跳过步骤 7 和 8。

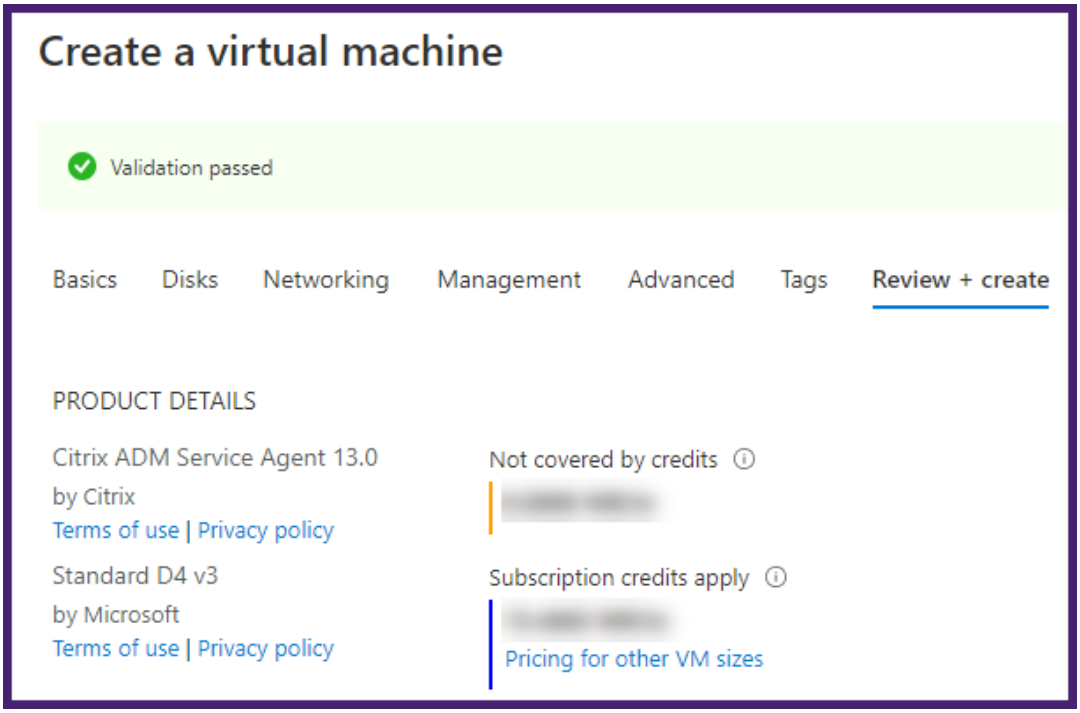
标记**:**

键入 NetScaler 代理标签的键值对。标签由区分大小写的键值对组成。这些标签使您能够轻松组织和识别代理。这些标签同时应用于 Azure 和 NetScaler Console。

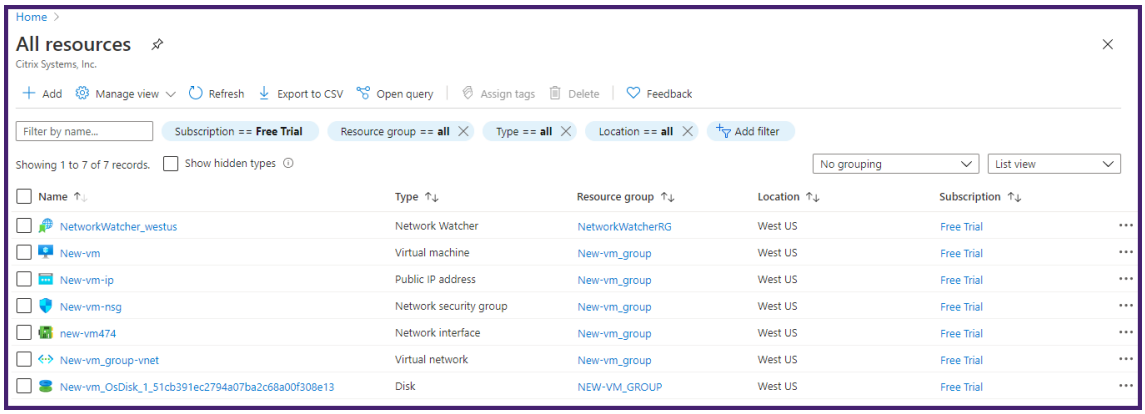


配置设置已验证，查看和创建 选项卡将显示验证结果。

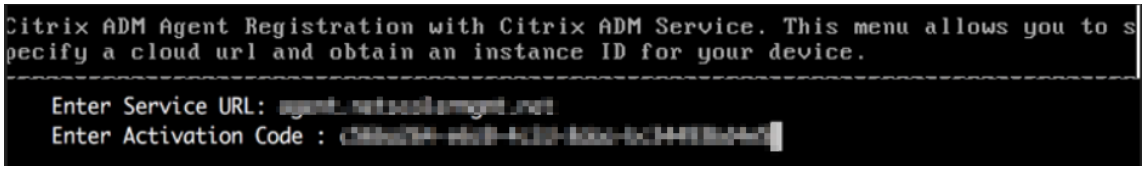
- 如果验证失败，此选项卡将显示失败的原因。返回到特定部分，并根据需要进行更改。
- 如果验证通过，请单击 创建。代理部署过程开始。



部署过程可能需要大约 10-15 分钟。成功完成部署后，您可以在 Microsoft Azure 帐户中查看 NetScaler 代理虚拟机。



6. 代理启动并运行后，使用 SSH 客户端登录到您的 NetScaler 代理。使用在虚拟机创建过程中指定的用户名和密码。
7. 在 shell 提示符下键入命令来运行部署脚本：**deployment_type.py**。
8. 按照入门 中的说明，输入您从 NetScaler 控制台的“设置代理”页面复制和保存的服务 **URL** 和 激活码。代理使用服务 URL 查找服务，并使用激活代码向服务注册。



代理注册成功后，代理程序将重新启动以完成安装过程。

代理重新启动后，访问 NetScaler Console，然后在“设置 代理”页面上的“已 发现的代理”下，验证代理的状态。

在 **Amazon Web Services (AWS)** 上安装 **NetScaler** 代理

January 29, 2024

NetScaler 代理充当 NetScaler 控制台与在数据中心或云端发现的实例之间的中介。

必备条件

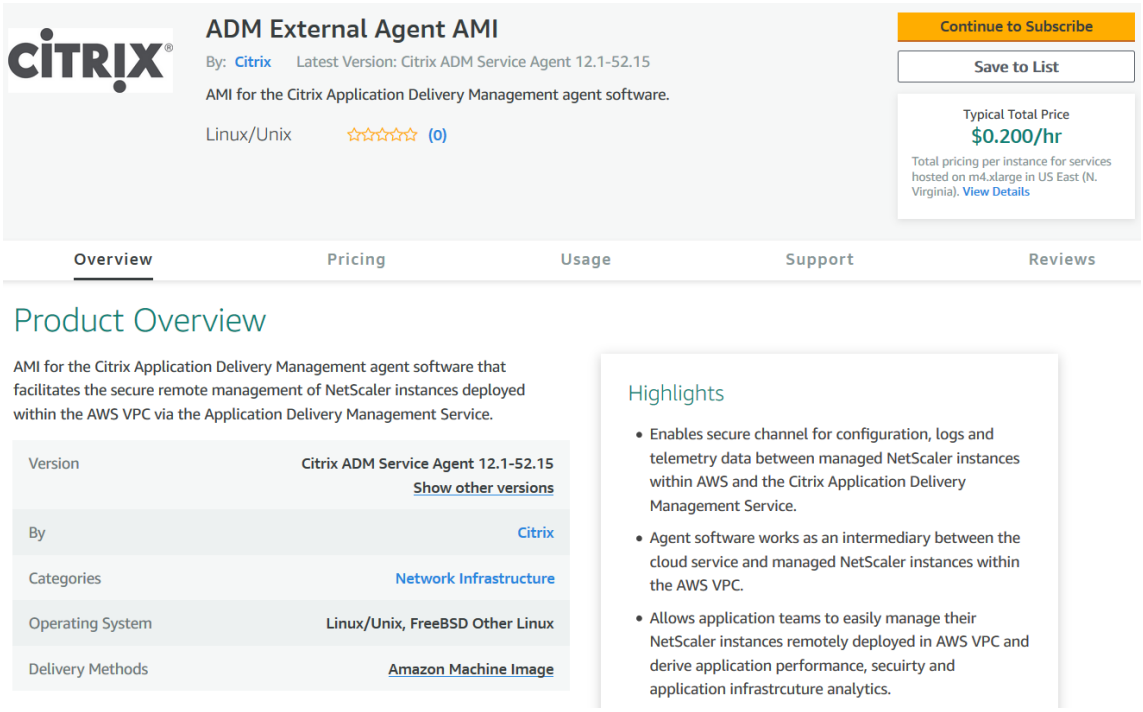
要使用 Amazon GUI 在 Amazon Web Services (AWS) 虚拟私有云 (VPC) 中启动 NetScaler 代理 AMI，您需要：

- AWS 帐户
- AWS 虚拟私有云 (VPC)
- IAM 帐户

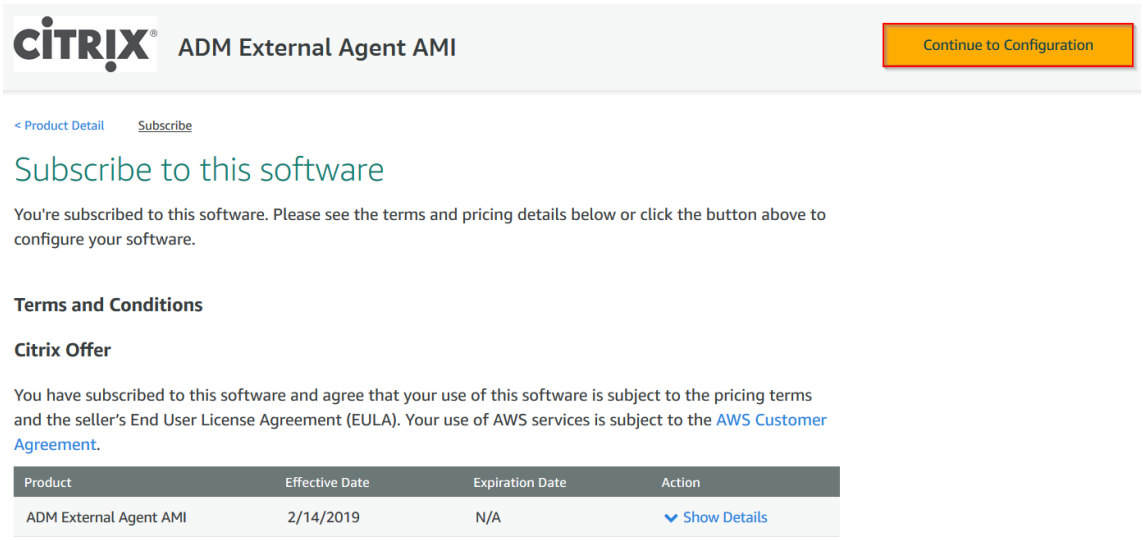
> 注意
>
> - 在配置 NetScaler 代理虚拟机之前，Citrix 建议创建安全组、虚拟专用网络、密钥对、子网和其他实体。因此，在预配过程中可以使用网络信息。
> - 要使 NetScaler 代理与 NetScaler 控制台和 NetScaler 实例进行通信，请确保推荐的端口处于打开状态。有关 NetScaler 代理的端口要求的完整详细信息，请参见端口。

要在 **AWS** 上安装 **NetScaler** 代理，请执行以下操作：

1. 使用 AWS 凭据登录 AWS 市场 。
2. 在搜索字段中，键入 **NetScaler** 代理以搜索 NetScaler 代理 AMI，然后单击开始。
3. 在搜索结果页面上，从可用列表中单击 **NetScaler** 控制台外部代理 **AMI**。
4. 在 **NetScaler** 控制台外部代理 **AMI** 页面上，单击“继续订阅”。



5. 订阅成功后，单击“继续配置”。



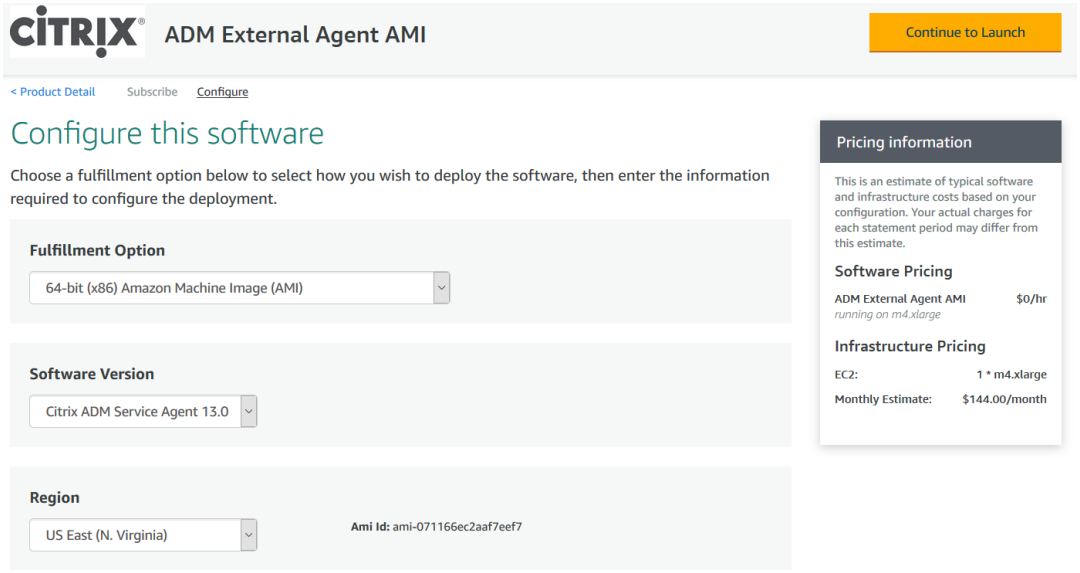
6. 在“配置此软件”页面上：

   a) 从 发货选项列表中选择 AMI。

   b) 从“软件版本”列表中选择最新的 NetScaler 代理版本。

   c) 从区域列表中选择您的 区域。

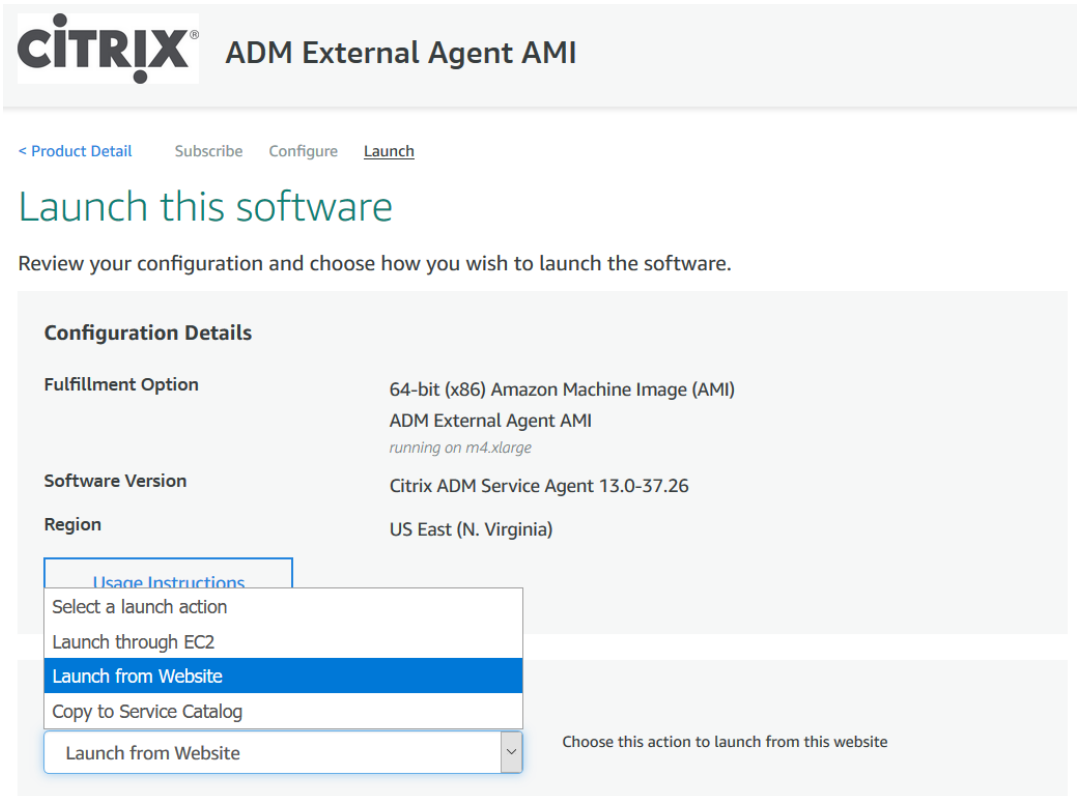
   d) 单击“继续”启动



7. 在“启动此软件”页面上，您可以通过两种方式注册 NetScaler 代理：

   a) 从网站启动

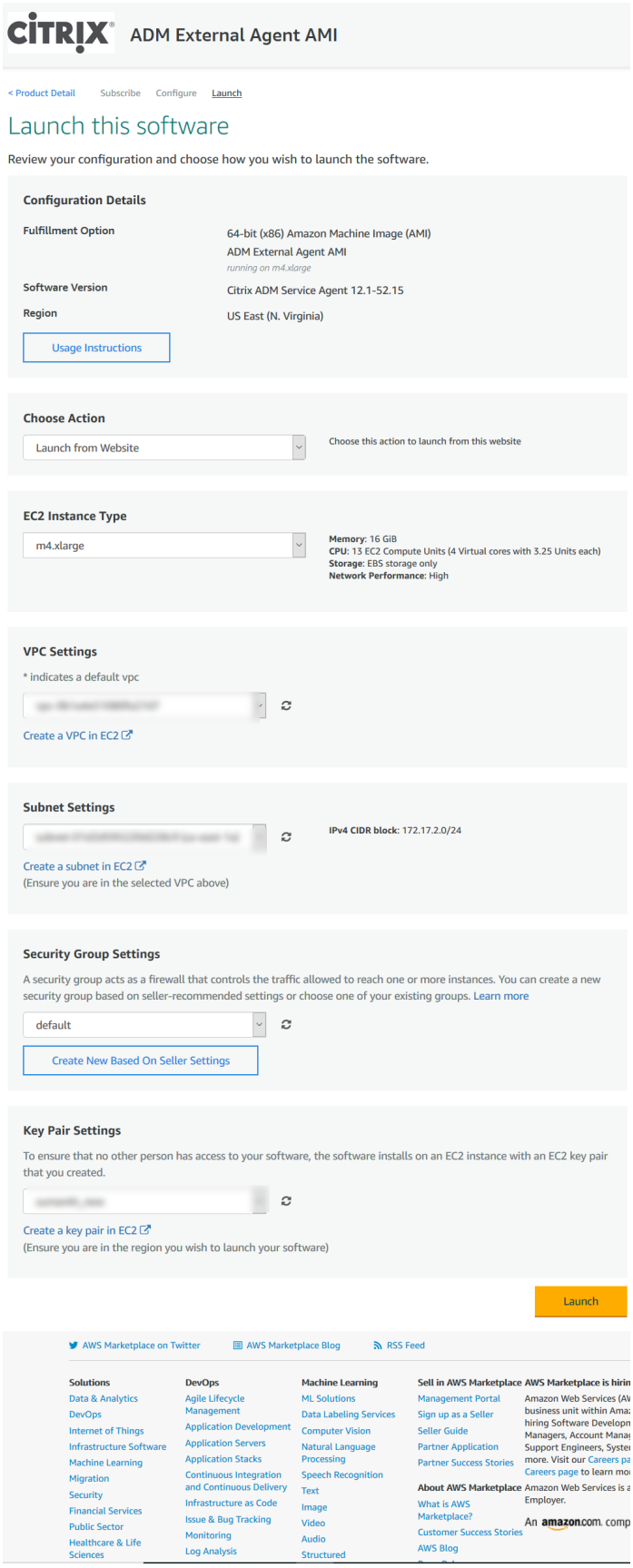
   b) 使用 **EC2** 启动



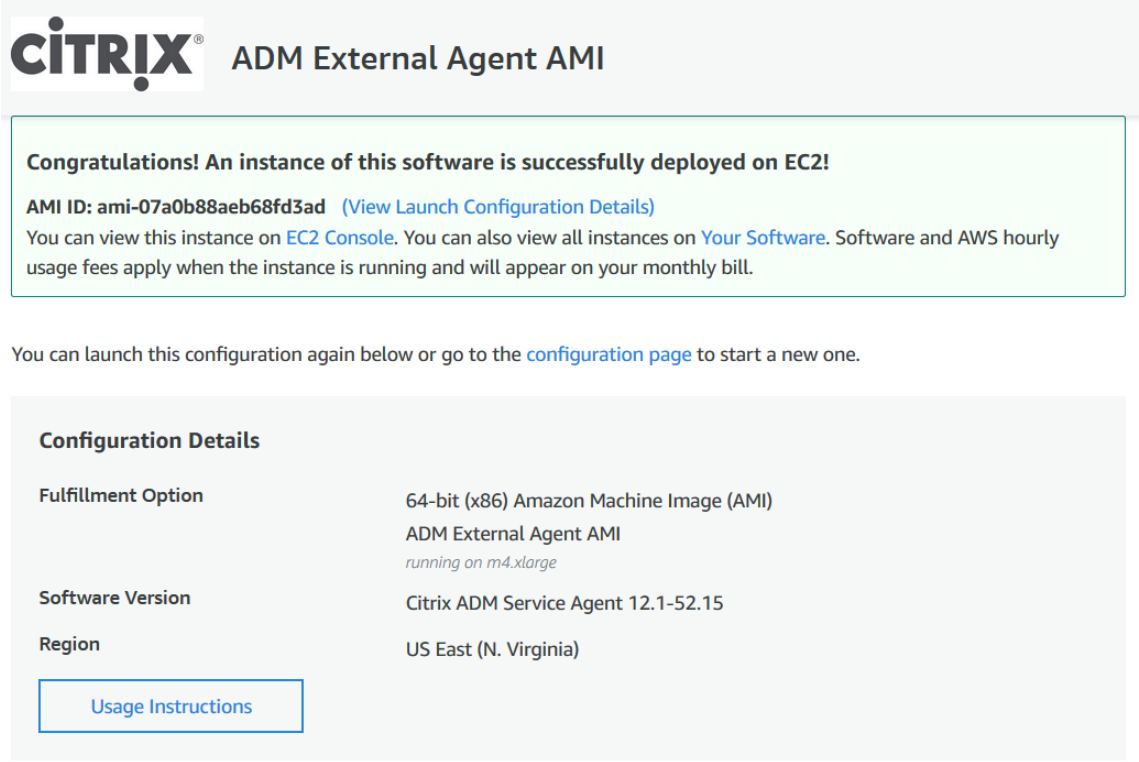
从网站启动

要从网站启动，请选择：

1. 来自 EC2 实例类型列表的 **EC2** 实例类型
2. 来自 VP **C** 设置 列表的 VPC。单击 **EC2** 中创建 **VPC** 为您的软件创建 VPC。
3. 子网 设置列表中的子网。选择 VPC 后，单击 **EC2** 中 创建子网以创建子网。
4. 来自安全组 设置列表的防火墙安全组。点击 根据卖家设置新 建以创建安全组。
5. 密钥对 设置列表中用于确保访问安全的密钥对。在 **EC2** 中单击创建密钥对 为您的软件创建密钥对。
6. 点击 启动



7. 从网站启动成功。



> 注意
>
> 部署过程可能需要大约 10-15 分钟。成功完成部署后，您可以在 AWS 帐户上查看 NetScaler 代理虚拟机。

8. 部署代理后，为您的 NetScaler 代理分配一个名称。
9. 代理启动并运行后，为您的 NetScaler 代理分配一个弹性 IP 地址。

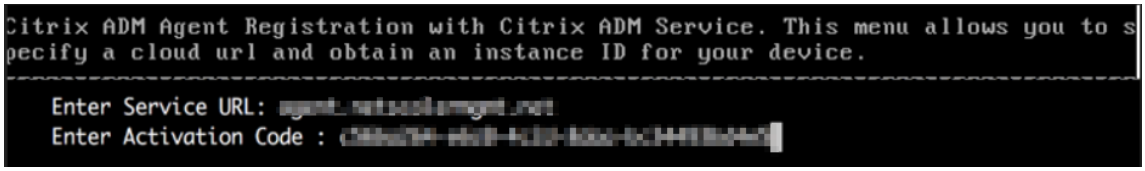
> 注意
>
> 弹性 IP 地址使 NetScaler 代理能够与 NetScaler 控制台进行通信。但是，如果您已将 NAT Gateway 配置为将流量路由到互联网，则可能不需要弹性 IP 地址。

10. 使用 SSH 客户端登录到您的 NetScaler 代理。

> 注
>
> 意：您可以使用以下方法之一登录到 NetScaler 代理：
>
> - 使用 `nsrecover` 作为用户名，使用 AWS 实例 ID 作为密码。
> - 使用 `nsroot` 作为用户名，使用有效的密钥对作为密码。

11. 输入以下命令以调用部署屏幕：部署类型**.py**

12. 按照“入门”中的说明，输入您从 NetScaler 控制台的“设置代理”页面复制和保存的 服务 **URL** 和 激活码。代理使用服务 URL 查找服务，并使用激活代码向服务注册。



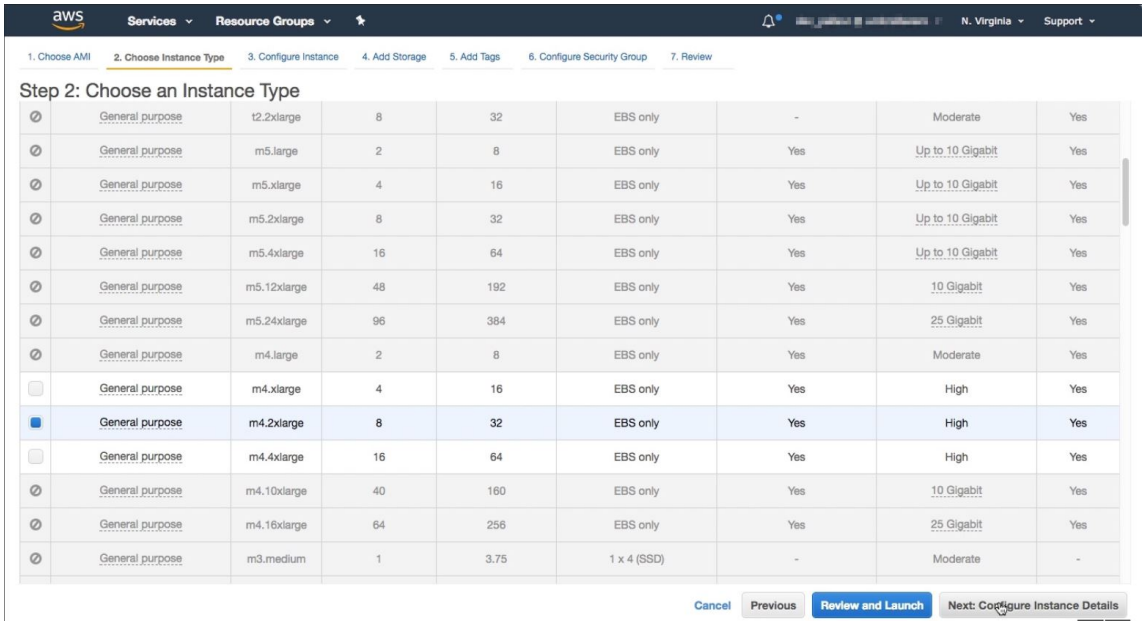
代理注册成功后，代理程序将重新启动以完成安装过程。

代理重新启动后，访问 NetScaler Console，然后在“设置 代理”页面上的“已 发现的代理”下，验证代理的状态。

使用 **EC2** 启动

要使用 EC2 启动，请从选择操作列表中 选择通过 EC2 启动，然后单击 启 动。

1. 在 选择实例类型 页面上，选择实例，然后单击 下一步：配置实例详细信息。



2. 在 配置实例详细信息 页面上，指定所需的参数。

   在“高级详细信息”部分下，您可以通过在 用户数据字段中指定身份验证详细信息或脚本来启用 零接触代理。

   - 认证详情 -按照“入门”中的说明指定您从 NetScaler 控制台的“设置代理”页面复制的 服务 **URL** 和 激活码。请按以下格式输入详细信息。

     ```
     registeragent -serviceurl <apigatewayurl> -activationcode <
         activationcodevalue>
     ```

     代理使用此信息在启动期间自动注册到 NetScaler 控制台。

   - 脚本 -将代理自动注册脚本指定为用户数据。以下是示例脚本：


```
#!/var/python/bin/python2.7
import os
import requests
import json
import time
import re
import logging
import logging.handlers
import boto3

'''
Overview of the Script:
The script helps to register a NetScaler agent with NetScaler Console. Pass it in userdata to make NetScaler agent in AWS to autoregister on bootup. The workflow is as follows
1)  Fetch the NetScaler Console API credentials (ID and secret) from AWS secret store (NOTE: you have to assign IAM role to the NetScaler agent that will give permission to fetch secrets from AWS secret store)
2)  Login to NetScaler Console with credentials fetched in step 1
3)  Call NetScaler Console to fetch credentials (serviceURL and token) for agent registration
4)  Calls registration by using the credentials fetched in step 3
'''

'''
These are the placeholders which you need to replace according to your setup configurations
aws_secret_id: Id of the AWS secret where you have stored NetScaler Console Credentials
The secrets value should be in the following json format
{
 "adm_user_id_key": "YOUR_ID", " adm_user_secret_key": " YOUR_SECRET" }

'''

aws_secret_id = "<AWS_secret_id>"
adm_ip_or_hostname = "<YOUR_ADM_POP>.adm.cloud.com"

'''
Set up a specific logger with your desired output level and log file name
'''
log_file_name_local = os.path.basename(\_\_file\_\_)
LOG_FILENAME = '/var/log/' + 'bootstrap' + '.log'
LOG_MAX_BYTE = 50\*1024\*1024
LOG_BACKUP_COUNT = 20

logger = logging.getLogger(\_\_name\_\_)
logger.setLevel(logging.DEBUG)
```



```
42  logger_handler = logging.handlers.RotatingFileHandler(
        LOG_FILENAME, maxBytes=LOG_MAX_BYTE, backupCount=
        LOG_BACKUP_COUNT)
43  logger_fortmater = logging.Formatter(fmt='%(asctime)-2s:%(
        funcName)30s:%(lineno)4d: [%(levelname)s] %(message)s',
        datefmt="%Y-%m-%d %H:%M:%S")
44  logger_handler.setFormatter(logger_fortmater)
45  logger.addHandler(logger_handler)
46
47  class APIHandlerException(Exception):
48      def \_\_init\_\_(self, error_code, message):
49          self.error_code = error_code
50          self.message = message
51
52      def \_\_str\_\_(self):
53          return self.message + ". Error code '" + str(self.
               error_code) + "'"
54
55  def parse_response(response, url, print_response=True):
56      if not response.ok:
57          if "reboot" in url:
58              logger.debug('No response for url: reboot')
59              resp = {
60  "errorcode": "500", "message": "Error while reading response.
        " }
61
62              return resp
63
64          if print_response:
65              logger.debug('Response text for %s is %s' % (url,
                    response.text))
66
67          response = json.loads(response.text)
68          logger.debug("ErrorCode - " + str(response['errorcode
               ']) + ". Message -" + str(response['message']))
69          raise APIHandlerException(response['errorcode'], str(
               response['message']))
70      elif response.text:
71          if print_response:
72              logger.debug('Response text for %s is %s' % (url,
                    response.text))
73
74          result = json.loads(response.text)
75          if 'errorcode' in result and result['errorcode'] > 0:
76              raise APIHandlerException(result['errorcode'],
                   str(result['message']))
77          return result
78
79  def _request(method, url, data=None, headers=None, retry=3,
        print_response=True):
80      try:
81          response = requests.request(method, url, data=data,
               headers=headers)
```



```
82              result = parse_response(response, url, print_response
                    =print_response)
83              return result
84          except [requests.exceptions.ConnectionError, requests.
                exceptions.ConnectTimeout]:
85              if retry > 0:
86                  return _request(method, url, data, headers, retry
                        -1, print_response=print_response)
87              else:
88                  raise APIHandlerException(503, 'ConnectionError')
89          except requests.exceptions.RequestException as e:
90              logger.debug(str(e))
91              raise APIHandlerException(500, str(e))
92          except APIHandlerException as e:
93              logger.debug("URL: %s, Error: %s, Message: %s" % (url
                    , e.error_code, e.message))
94              raise e
95          except Exception as e:
96              raise APIHandlerException(500, str(e))
97
98      try:
99          '''Get the AWS Region'''
100         client = boto3.client('s3')
101         my_region = client.meta.region_name
102         logger.debug("The rgion is %s" % (my_region))
103
104         '''Creating a Boto cleint session'''
105         session = boto3.session.Session()
106         client = session.client(
107             service_name='secretsmanager',
108             region_name=my_region
109         )
110
111         '''Getting the values stored in the secret with id: <
                aws_secret_id>'''
112         get_id_value_response = client.get_secret_value(
113             SecretId = aws_secret_id
114         )
115         adm_user_id = json.loads(get_id_value_response["
                SecretString"])["adm_user_id_key"]
116         adm_user_secret = json.loads(get_id_value_response["
                SecretString"])["adm_user_secret_key"]
117
118     except Exception as e:
119         logger.debug("Fetching of NetScaler Console credentials
                from AWS secret failed with error: %s" % (str(e)))
120         raise e
121
122     '''
123     Initializing common NetScaler Console API handlers
124     '''
125     mas_common_headers = {
126
```

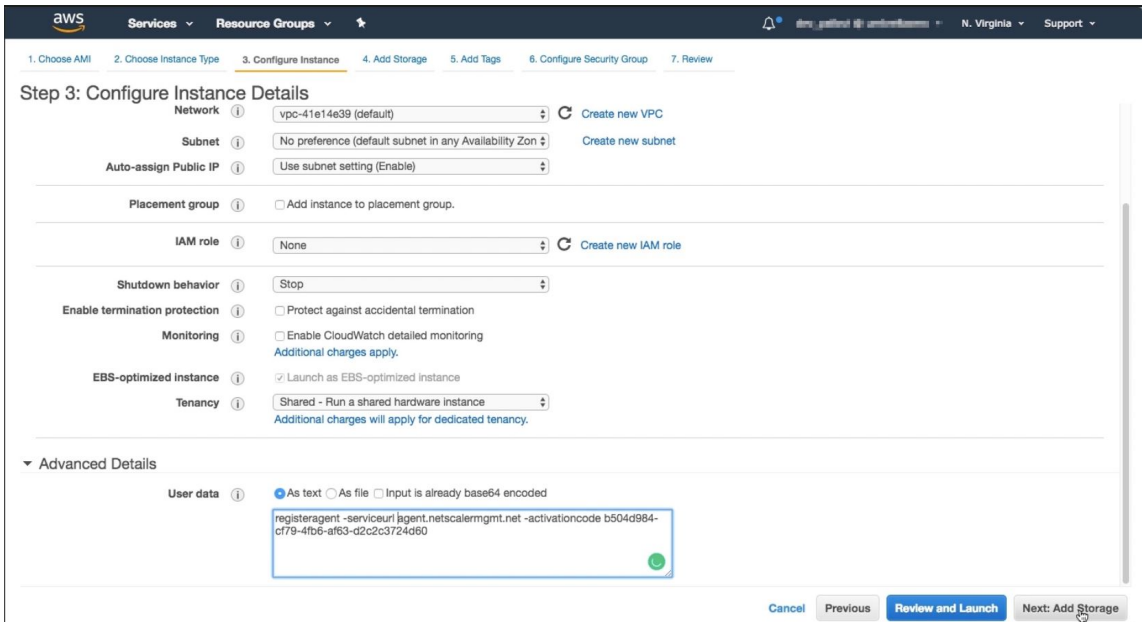


```
127         'Content-Type': "application/json",
128         'Accept-type': "application/json",
129         'Connection': "keep-alive",
130         'isCloud': "true"
131      }
132
133
134     '''
135     API to login to the NetScaler Console and fetch the Session
            ID and Tenant ID
136     '''
137     url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
            config/login"
138     payload = 'object={
139     "login":{
140     "ID":"' + adm_user_id + '","Secret":"' + adm_user_secret + '"
            }
141      }
142     '
143     try:
144         response = _request("POST", url, data=payload, headers=
                mas_common_headers)
145         sessionid = response["login"][0]["sessionid"]
146         tenant_id = response["login"][0]["tenant_name"]
147     except Exception as e:
148         logger.debug("Login call to the NetScaler Console failed
                with error: %s" % (str(e)))
149         raise e
150
151     '''
152     API to fetch the service URL and Token to be used for
            registering the agent with the NetScaler Console
153     '''
154     mas_common_headers['Cookie'] = 'SESSID=' + str(sessionid)
155     url = "https://" + str(adm_ip_or_hostname) + "/nitro/v1/
            config/trust_preauthtoken/" + tenant_id +"?customer="+
            tenant_id
156     logger.debug("Fetching Service URL and Token.")
157     try:
158         response = _request("GET", url, data=None, headers=
                mas_common_headers)
159         service_name  = response["trust_preauthtoken"][0]["
                service_name"]
160         token = response["trust_preauthtoken"][0]["token"]
161         api_gateway_url = response["trust_preauthtoken"][0]["
                api_gateway_url"]
162     except Exception as e:
163         logger.debug("Fetching of the Service URL Passed with
                error. %s" % (str(e)))
164         raise e
165
166     '''
167     Running the register agent command using the values we
```



```
        retrieved earlier
168     '''
169     try:
170         registeragent_command = "registeragent -serviceurl "+
                api_gateway_url+" -activationcode "+service_name+";"+
                token
171         file_run_command = "/var/python/bin/python2.7 /mps/
                register_agent_cloud.py "+registeragent_command
172         logger.debug("Executing registeragent command: %s" % (
                file_run_command))
173         os.system(file_run_command)
174     except Exception as e:
175         logger.debug("Agent Registeration failed with error: %s"
                % (str(e)))
176             raise e
```

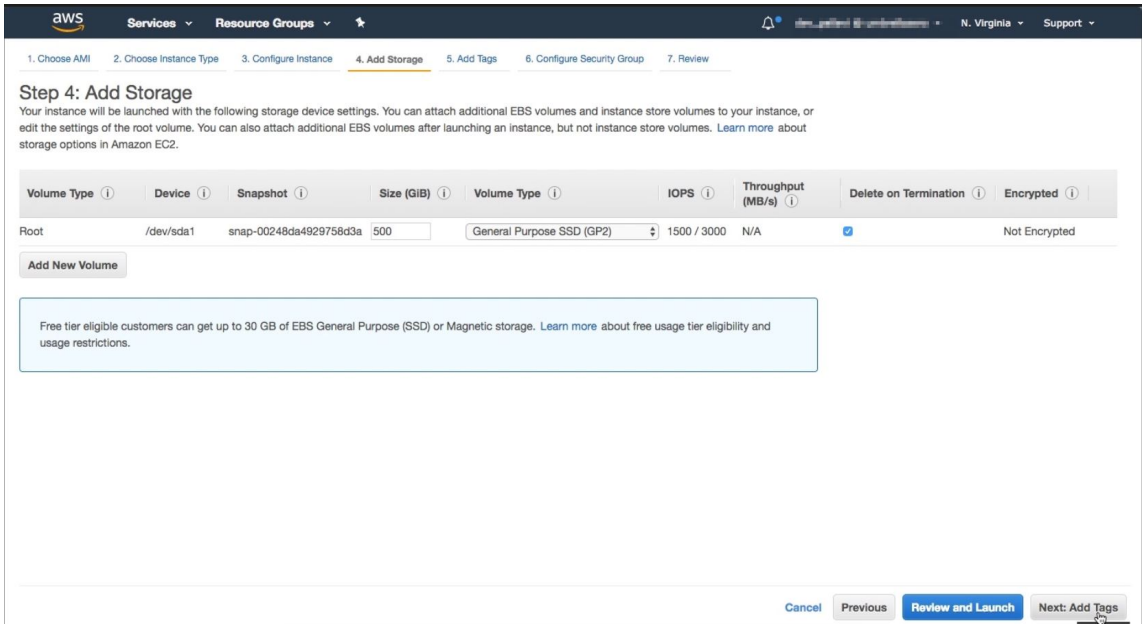
此脚本从 AWS 机密管理器获取认证详情，并deployment.py运行 脚本将代理注册到 NetScaler 控制台。



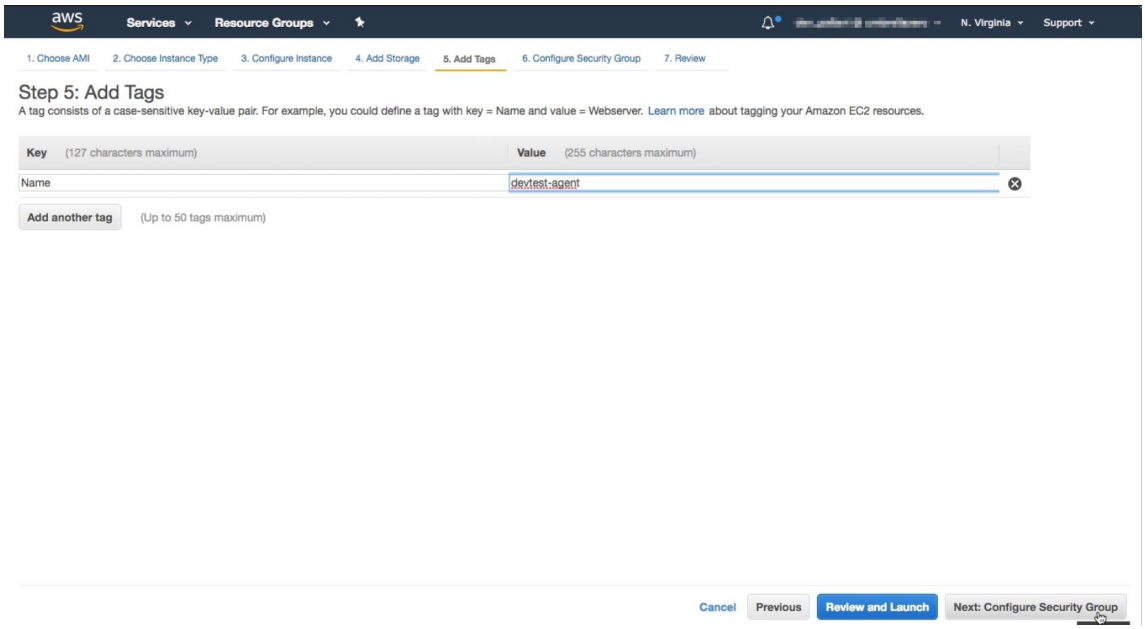
> 注意
>
> 虽然您可以自动分配公有 IP 地址，但也可以分配弹性 IP 地址。如果未配置 NAT Gateway，则需要分配弹性 IP 地址。
>
> 如果此步骤中未设置弹性 IP 地址，您仍然可以在 EC2 控制台上进行设置。您可以创建新的弹性 IP 地址，并使用实例 ID 或 ENI-ID 将其与 NetScaler 代理关联。

单击 添加存储空间。

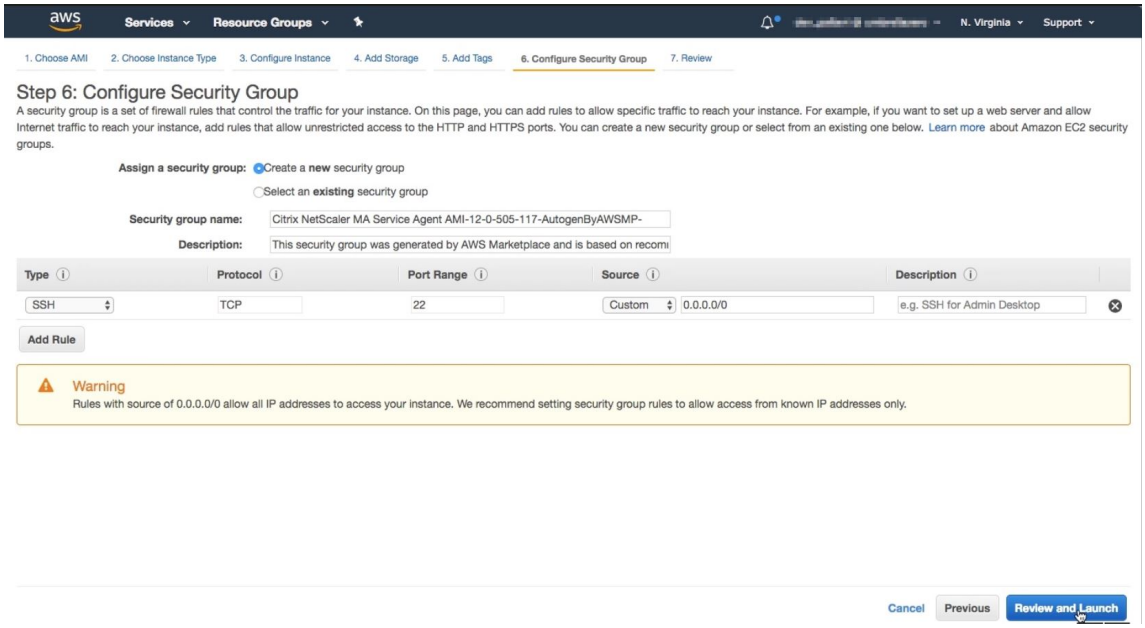
3. 在 添加存储 页面上，配置实例的存储设备设置，然后单击 下一步：添加标签。



4. 在 添加标签 页面上，定义实例的标签，然后单击 下一步：配置安全组。

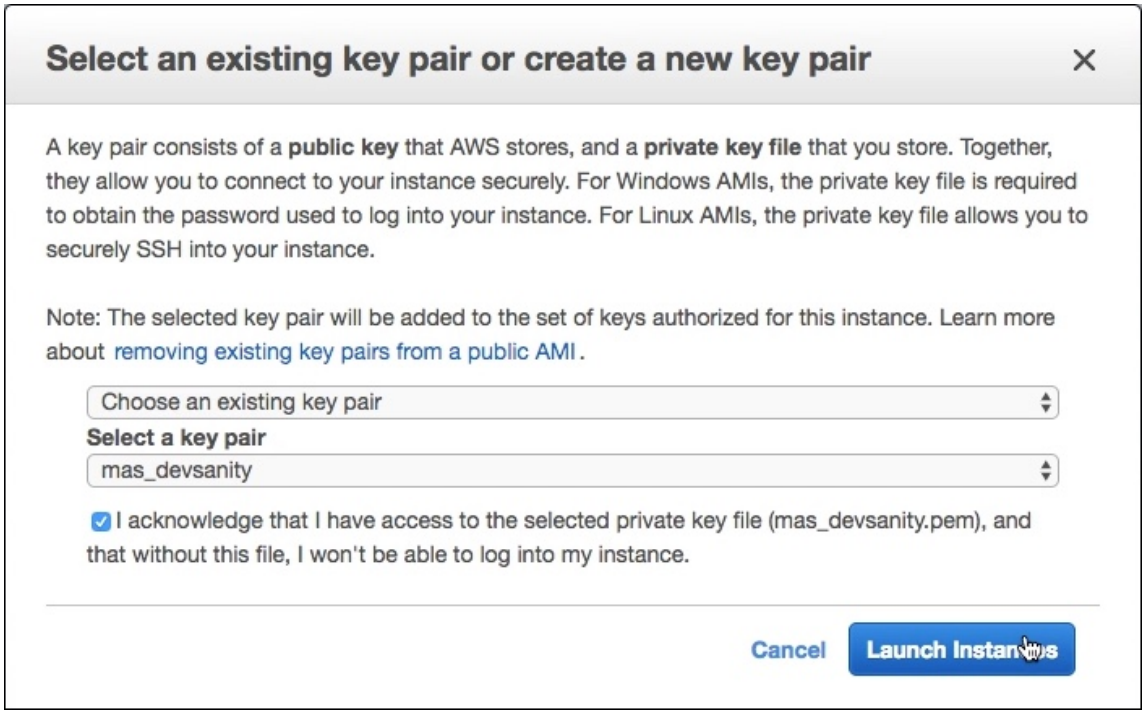


5. 在 配置安全组 页面上，添加允许特定流量进入实例的规则，然后单击 查看并启动。



6. 在 查看实例启动 页面上，查看实例设置，然后单击 启动。
7. 在 选择现有密钥对或创建新密钥对对 话框中，创建密钥对。您还可以从现有密钥对中进行选择。

   接受确认，然后单击 启动实例。



部署过程可能需要大约 10-15 分钟。成功完成部署后，您可以在 AWS 帐户上查看 NetScaler 代理虚拟机。

在 **GCP** 上安装 **NetScaler** 代理

January 29, 2024

NetScaler 代理充当 NetScaler 控制台与在数据中心或云端发现的实例之间的中介。您可以在 Google Cloud Platform (GCP) 上部署代理，以便利通过 NetScaler 控制台安全远程管理部署在谷歌云虚拟网络中的 NetScaler 实例。如需更多信息，请查看 Google Cloud Platform Marketplace（Google 云端平台市场）。

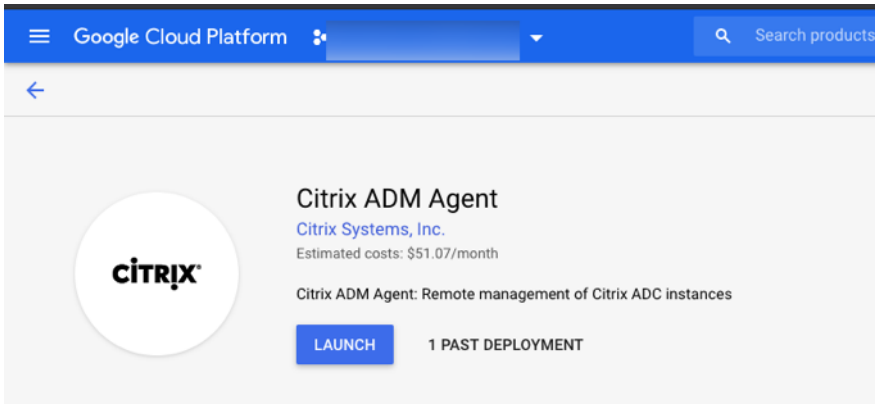
必备条件

要在 GCP 上安装 NetScaler 代理，您需要一个 GCP 帐户。

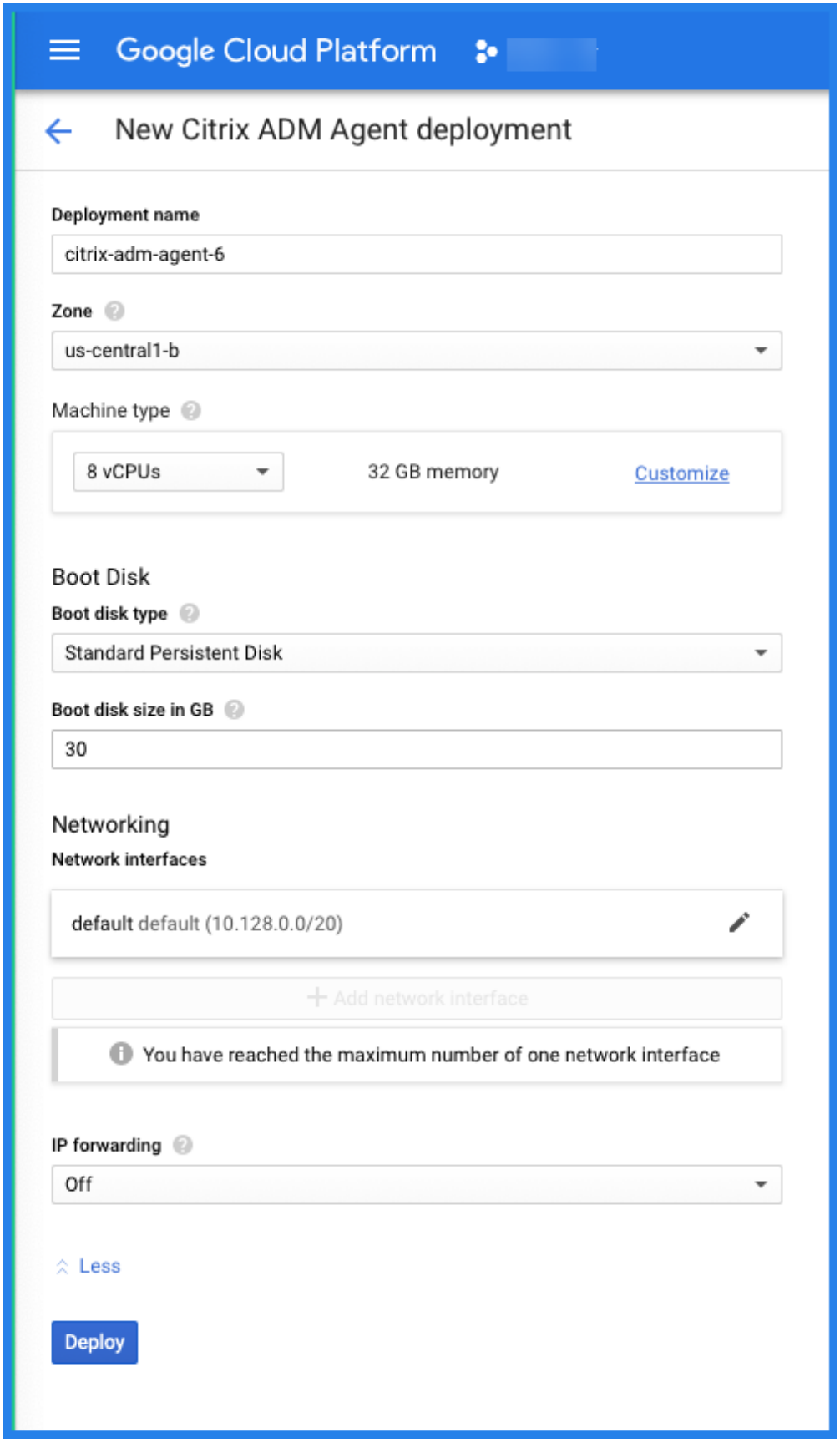
在 **GCP** 上安装 **NetScaler** 代理

按照以下步骤在 GCP 上安装 NetScaler 代理。

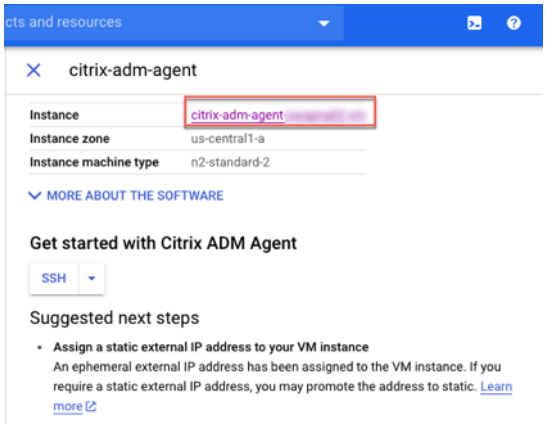
1. 使用您的凭据登录 GCP 控制台（console.cloud.google.com），然后进入市场。
2. 在搜索字段中，键入 **NetScaler** 代理。
3. 在结果字段中单击 **NetScaler** 代理，然后单击“** 启动”。



4. 在新的 **NetScaler** 代理 部署页面中，大部分选项都是默认设置的。您可以根据需要更改默认配置，然后单击 部署。



5. 部署代理后，单击实例链接，然后在 虚拟机实例详细信息页面中查看详细信息。

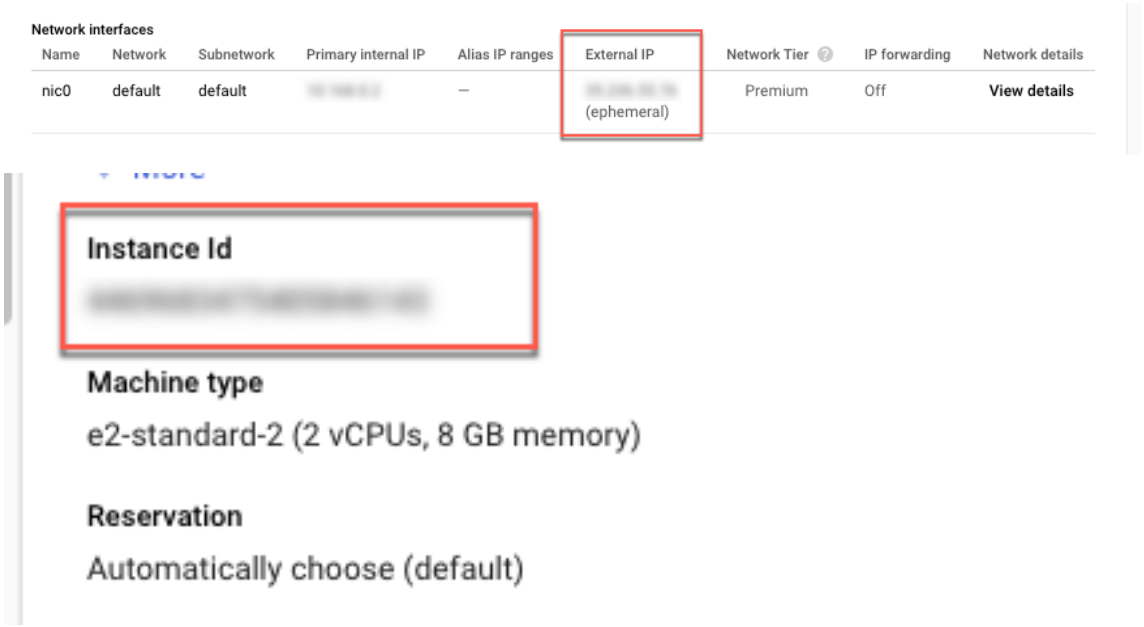


6. 使用代理外部 IP 地址通过 SSH 客户端登录代理。使用以下命令：

```
ssh nsrecover@<external IP address of the agent>
```

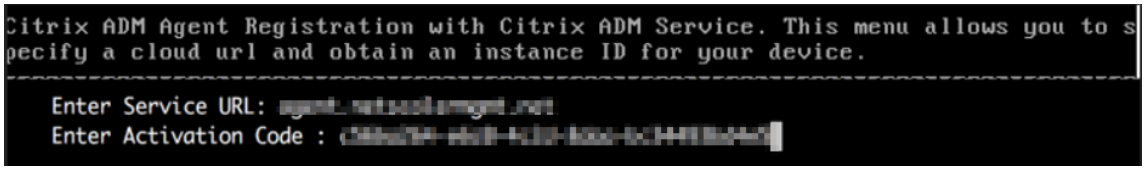
密码：实例 ID

您能在 虚拟机实例详细信息页面 中找到外部 **IP** 地址和实例 ID 吗?



7. 输入以下命令以调用部署屏幕：部署类型**.py**

8. 按照“入门”中的说明，输入您从 NetScaler 控制台的“设置代理”页面复制和保存的 服务 **URL** 和 激活码。代理使用服务 URL 查找服务，并使用激活代码向服务注册。



代理注册成功后，代理程序将重新启动以完成安装过程。

代理重新启动后，访问 NetScaler Console，然后在“设置 代理”页面上的“已 发现的代理”下，验证代理的状态。

使用 YAML 在 Kubernetes 群集中安装 NetScaler 代理

January 29, 2024

> 注意
>
> 将代理作为微服务安装的过程可在“入门”部分中找到。

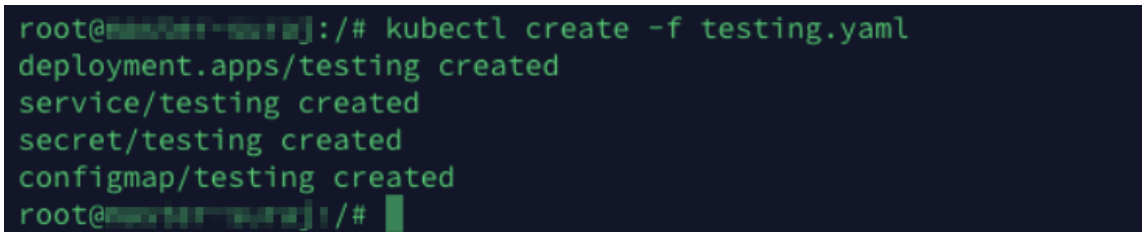
在 Kubernetes 主节点中：

1. 保存下载的 YAML 文件
2. 请运行以下命令：

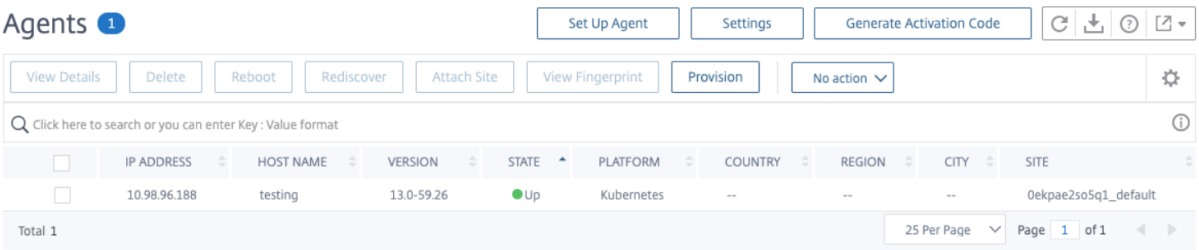
   ```
   kubectl create -f <yaml file>
   ```

   例如，`kubectl create -f testing.yaml`

   代理已成功创建。

在 NetScaler 控制台中，导航 到基础架构 > 实例 代理以查看代理状态。



> 注意：
>
> 在 Kubernetes 群集中使用 YAML 配置的 NetScaler 代理支持自动代理升级（常青升级）。

使用 **OpenShift** 控制台安装 **NetScaler** 代理操作员

April 10, 2024

操作员是一个开源工具包，使您能够以有效、自动和可扩展的方式部署和管理 Kubernetes 应用程序。作为管理员，您可以使用 **NetScaler ADM** 代理操作员在 **OpenShift** 群集中部署代理。

> 注意：
>
> 默认情况下，在 OpenShift 群集中配置的代理不会自动升级。

必备条件

在部署之前，请确保：

- 您拥有特权安全上下文约束来控制 Pod 的权限。对于代理，运行以下命令以获取服务帐号的权限安全上下文限制：

  ```
  oc adm policy add-scc-to-user privileged -z adm-agent-serviceaccount
  ```

- 运行以下命令创建代理登录密钥：

  ```
  kubectl create secret generic admlogin --from-literal=username=
  nsroot --from-literal=password=<adm-agent-password> -n <namespace
  >
  ```

  > 注意：
  >
  > - `<adm-agent-password>` 是一个密码示例。您必须为代理设置密码，NetScaler CPX 使用这些凭据向代理注册。
  > - 创建实例时，在代理 YAML 中为 `loginSecret` 提供 **admlogin**。

  如果您在不同的命名空间中部署 NetScaler CPX 和代理，请确保：

  - 使用在其中部署了 NetScaler CPX 的 `citrix-cpx=enabled` 的标签命名空间。
  - 安装代理操作员时设置为 `helper.required` true 或 false。

    > 注意：
    >
    > 默认情况下，`helper.required` 设置为 **false**。如果此参数设置为 false，则如果 NetScaler CPX 和代理位于不同的命名空间中，则必须确保在每个命名空间中创建 **admlogin** 密钥。

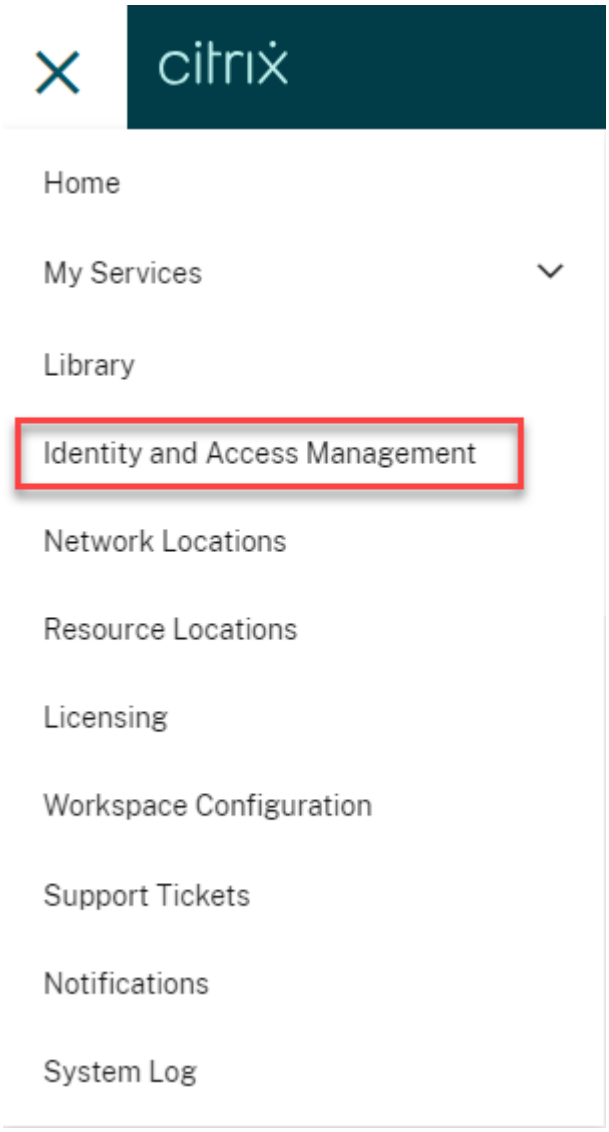
- 这是`accessSecret`代理 YAML 中必需的。代理需要这些凭据才能连接到 NetScaler 控制台服务。


```
kubectl create secret generic <secretname> --from-literal=accessid
=<ID> --from-literal=accesssecret=<Secret> -n namespace
```

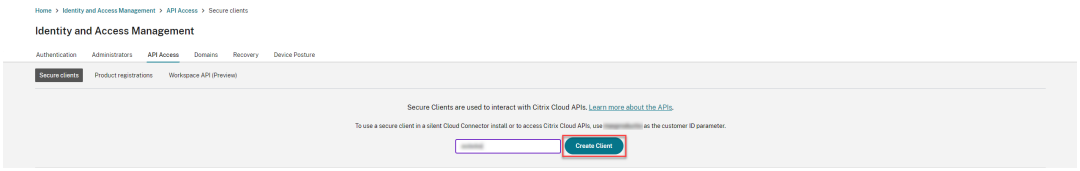
> 注意：
>
> 创建实例时，在代理 YAML 中为 accessSecret 提供密钥名称。

您可以通过以下步骤获取访问 NetScaler 控制台的访问 ID 和密钥：

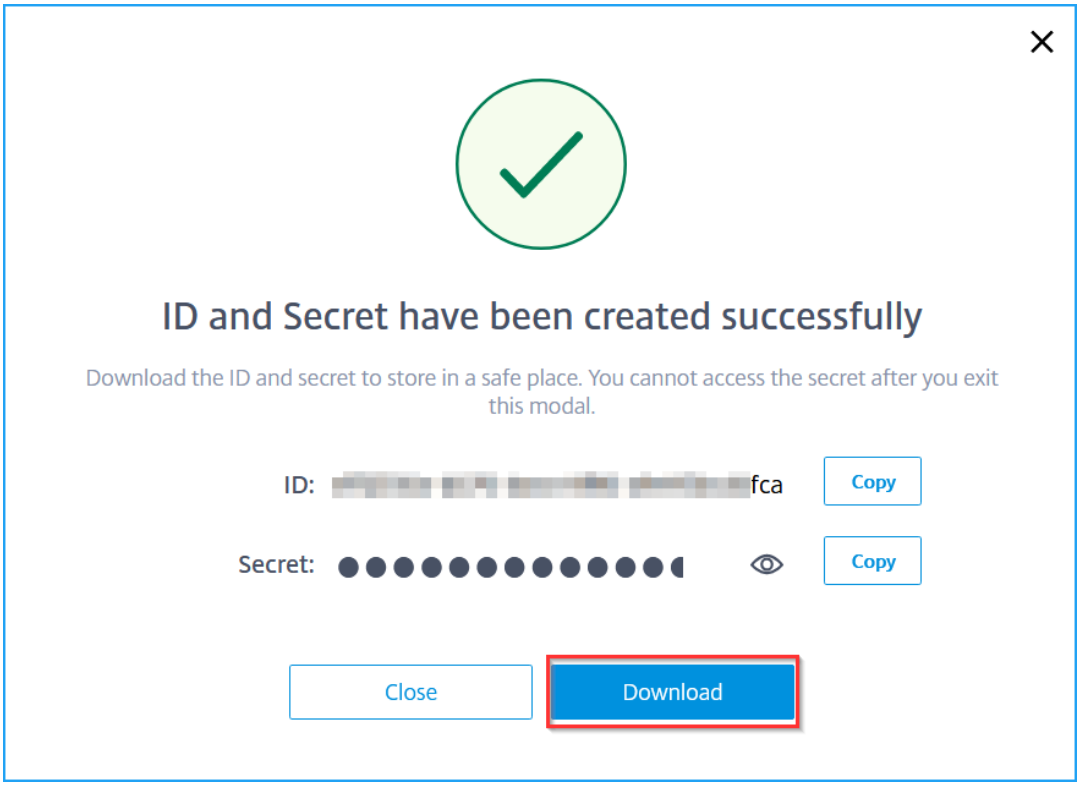
1. 登录 Citrix Cloud 管理控制台。
2. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。



3. 在 **API** 访问 选项卡中，输入安全客户端名称，然后单击 创建客户端。

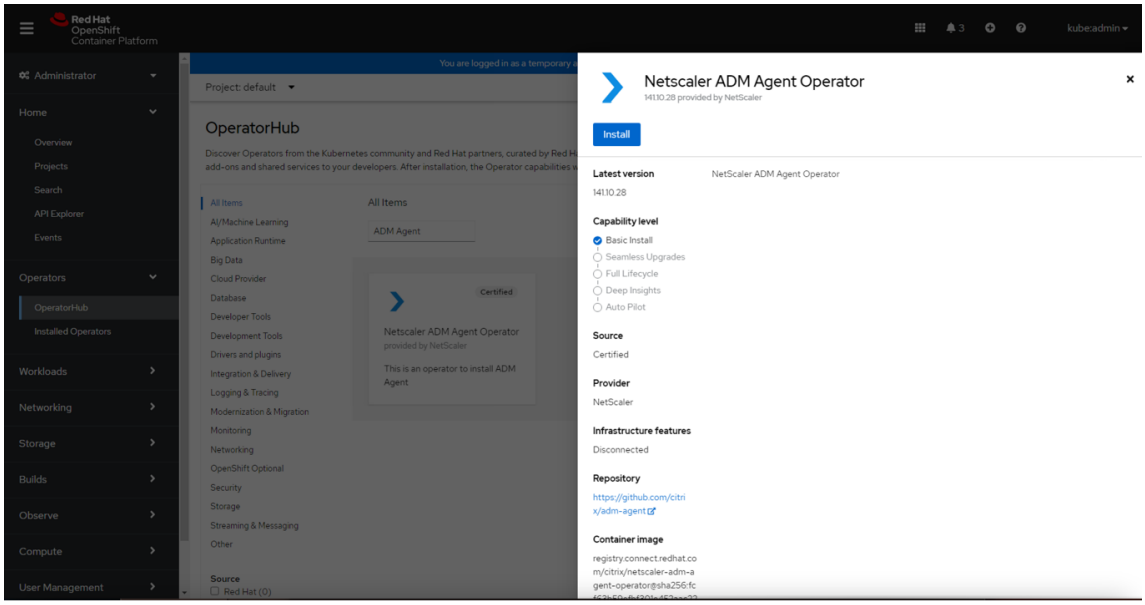


4. ID 和密钥已生成。单击“下载”并保存 CSV 文件。



安装代理操作员

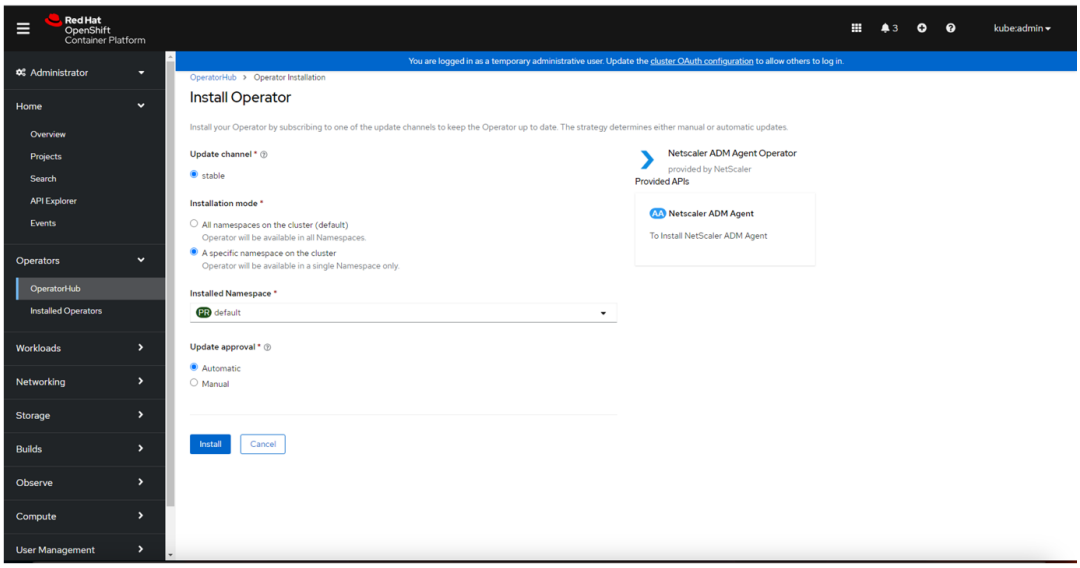
1. 登录 OpenShift 群集控制台。
2. 导航到 操作员 **> OperatorHub**。
3. 在搜索栏中，提供代理名称并选择 **NetScaler ADM** 代理操作员，然后单击“安装”。



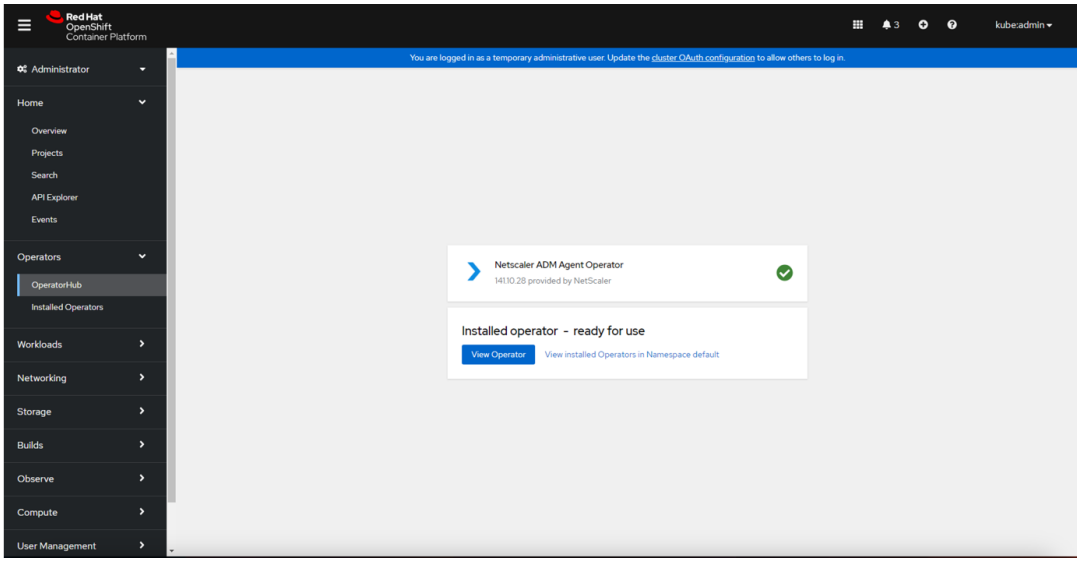
4. 在“安装操作员”页面中，有两个选项：

   - 群集上的所有命名空间（默认） - 允许代理操作员订阅群集中所有可用的命名空间，并允许您从群集上的任何命名空间启动代理操作员实例。
   - 群集上的特定命名空间 -允许代理操作员订阅群集上的选定命名空间，并且您只能从所选命名空间启动代理操作员实例。

     在此示例中，代理运算符被分配给一个名为 Defa ult 的命名空间。在“更新批准”下选择“自动”，然后单击“安装”。

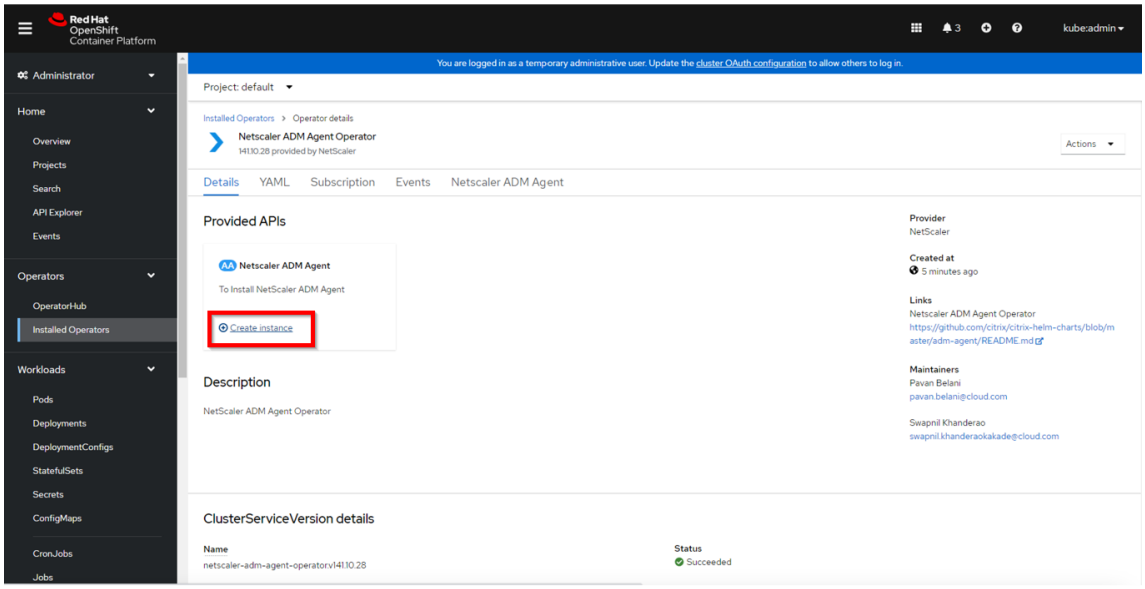


   等待代理操作员成功订阅。



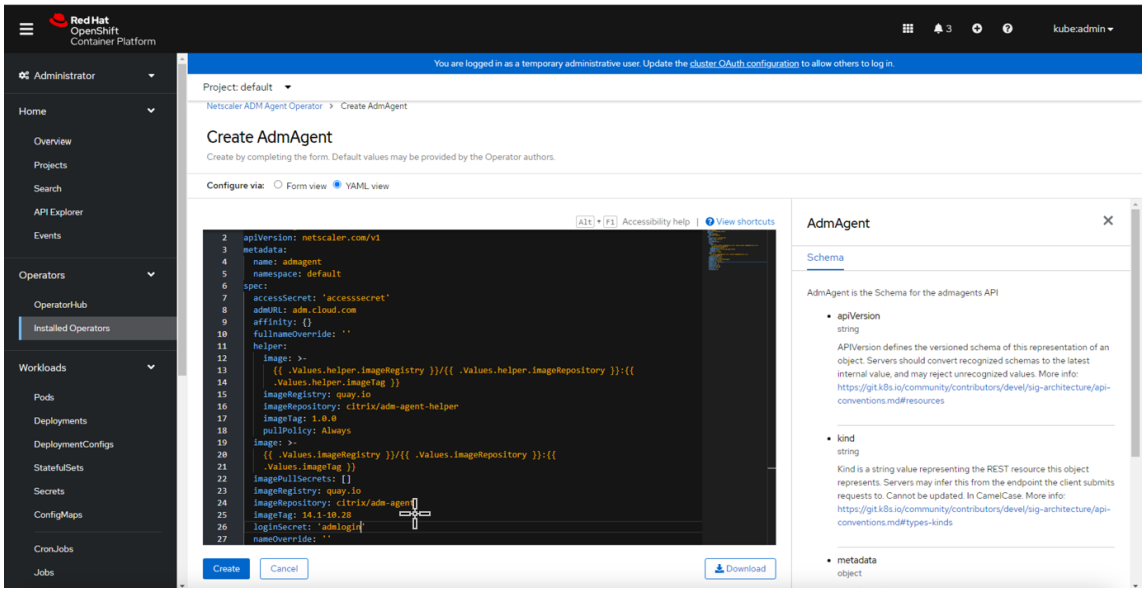
5. 导航到“工作负载”**>**“容 器”，然后验证 `netscaler-adm-agent-operator-controller` Pod 是否已启动并
   正在运行。

6. Pod 启动并运行后，单击“创建实例”。

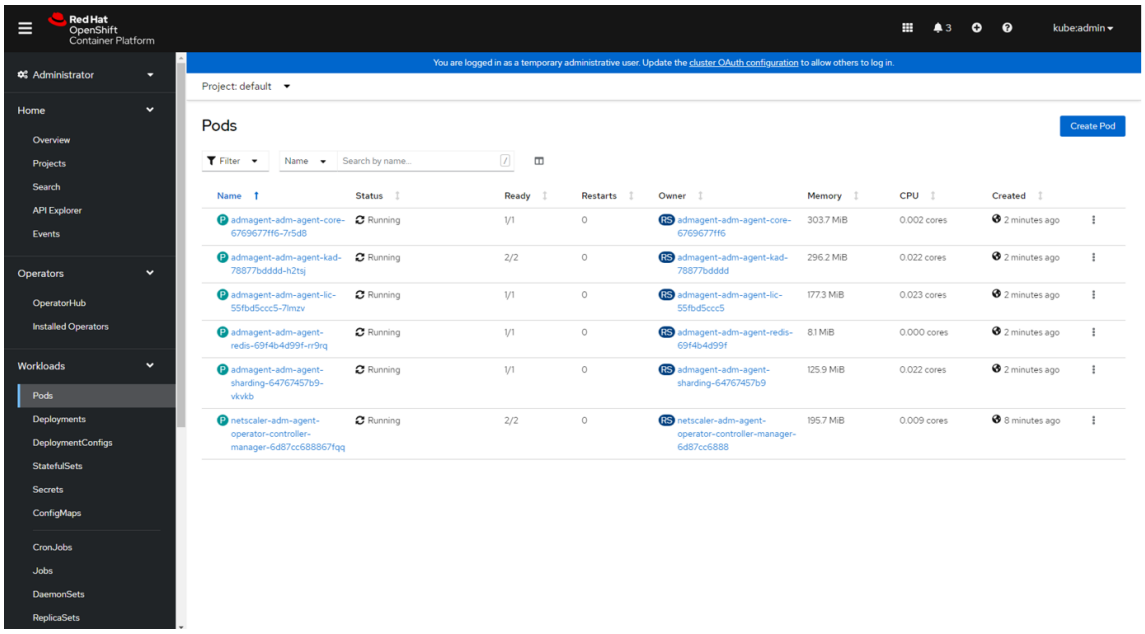


7. 选择 **YAML** 视图 以更新任何参数，然后单击“创建”。

> 注意：
>
> 确保每个 OpenShift 群集只能有一个代理实例。

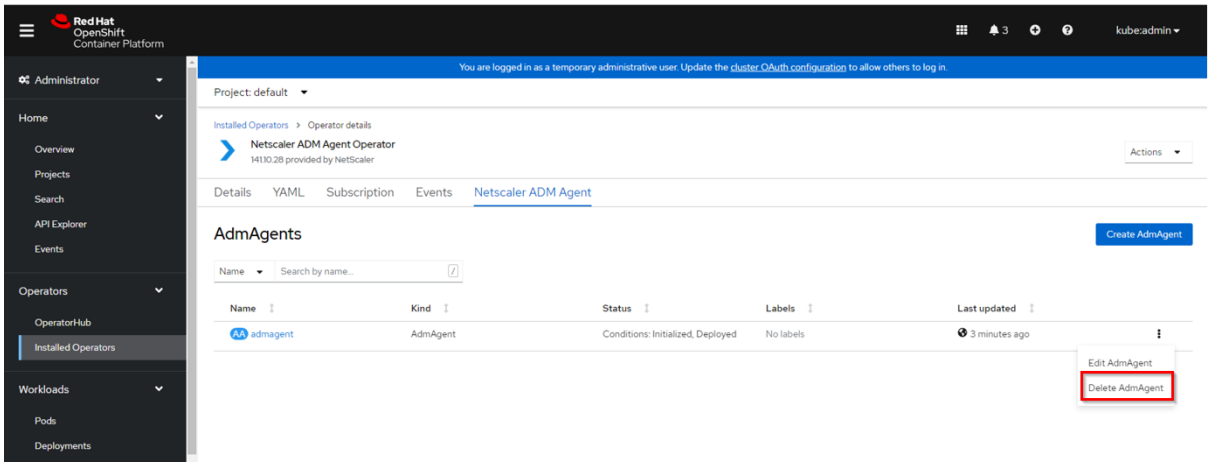


8. 导航到“工作负载”“容器”，确保代理容器已启动并运行。



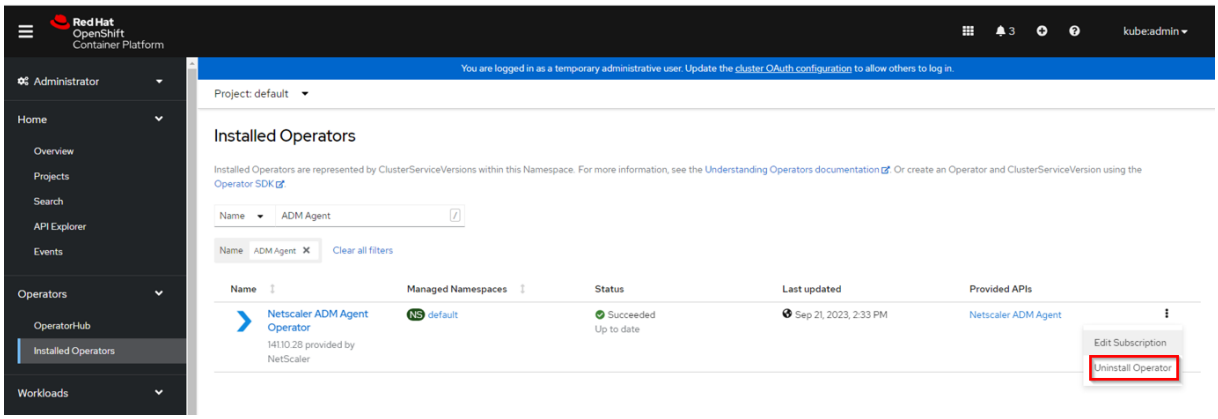
删除代理实例

您可以导航到操作员 **>** 已安装的操作员，从群集中删除代理实例。在 **NetScaler ADM** 代理操作员选项卡中，选择实例，然后从列表中选择删除 **AdmAgent**。



卸载代理操作员

如果要从群集中卸载代理操作员窗格，请导航到 操作员 **>** 已安装的操作员，然后从列表中选择 卸载操作员。



使用 **Helm Charts** 安装基于容器的代理

January 29, 2024

您可以部署基于容器的代理，将 NetScaler CPX 与 NetScaler 控制台连接起来，以管理和监视 NetScaler CPX。要部署基于容器的代理，请按照本文档中提供的步骤进行操作。

> 注意：
>
> 默认情况下，基于容器的代理不会自动升级（常青升级）。

如何获取帮助和支持

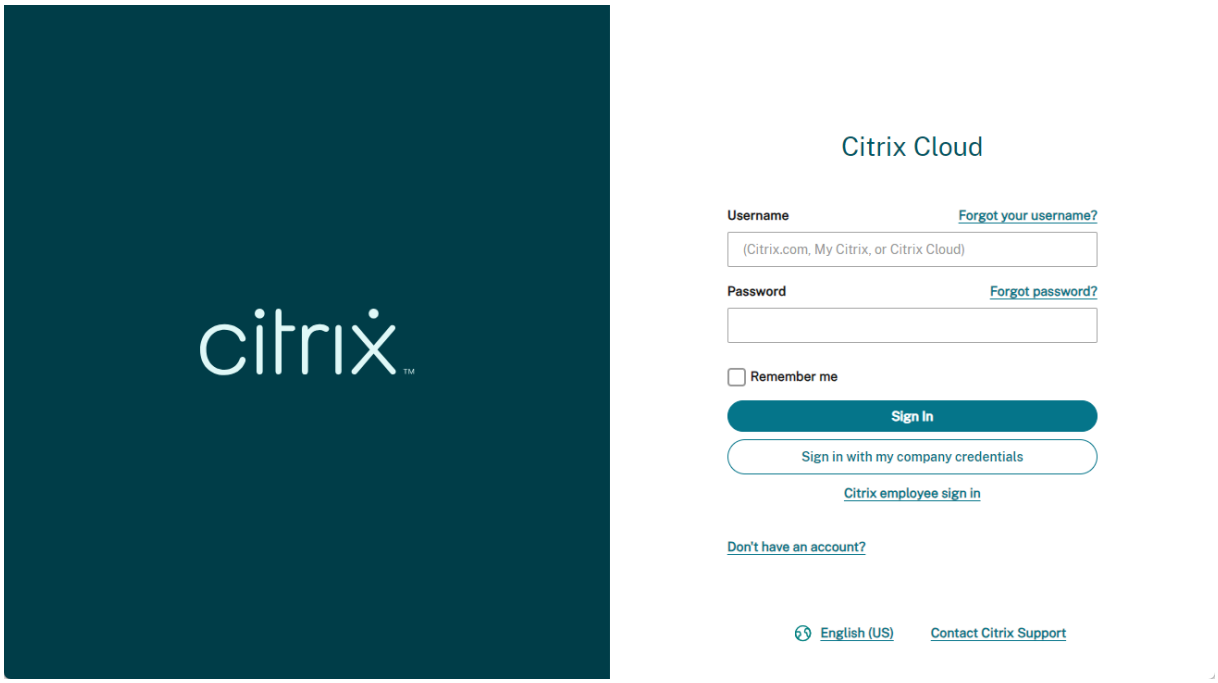
July 17, 2024

作为 Citrix Cloud 用户，有时您可能需要帮助以确保我们的基础架构的顺利运行。本主题提供有关不同帮助和支持选项以及如何访问这些选项的详细信息。

创建 **Citrix Cloud** 帐户

如果您在注册 Citrix Cloud 帐户时遇到错误，请联系 Citrix 客户服务。

登录您的帐户



如果您在登录到 Citrix Cloud 帐户时遇到麻烦，请执行以下操作：

- 确保使用注册帐户时提供的电子邮件地址和密码登录。
- 在以下情况下，Citrix Cloud 会自动提示您在登录之前重置密码：
  - 您已经有一段时间没有登录 Citrix Cloud 了
  - 您的密码不符合 Citrix Cloud 的要求
- 有关更多信息，请参阅本文中的 更改密码 。

- 如果您的公司允许用户使用其公司凭据而不是 Citrix 帐户登录 Citrix Cloud，请单击“使用我的公司凭据登录”，然后输入贵公司的登录 URL。然后可以输入您的公司凭据以访问贵公司的 Citrix Cloud 帐户。如果您不知道贵公司的登录 URL，请联系贵公司的管理员以获得帮助。

更改密码

如果您忘记了 Citrix Cloud 帐户密码，请单击 忘记用户名或密码?，然后您可以输入帐户的电子邮件地址。您会收到重置密码的电子邮件。如果您没有收到密码重置电子邮件，或者需要更多帮助，请联系 Citrix 客户服务。

为了帮助您确保帐户密码的安全，Citrix Cloud 可能会在您尝试登录时提示您重置密码。在以下情况下会出现此提示：

- 您的密码不符合 Citrix Cloud 的复杂性要求。密码长度必须至少为 8 个字符，并包括：
  - 至少有一个数字
  - 至少包含一个大写字母
  - 至少一个符号：! @ # $ % ^ * ? + = -
- 您的密码包含字典中的单词。
- 您的密码列在已知的泄露密码数据库中。
- 在过去的六个月中，您没有登录 Citrix Cloud。

出现提示时，选择“重置密码”为您的帐户创建一个新的强密码。

Citrix Cloud 支持论坛

在 Citrix Cloud 支持论坛 上，您可以获得帮助、提供反馈和改进建议、查看其他用户的对话或开始自己的话题。

NetScaler 支持人员会跟踪这些论坛并随时准备回答您的问题。其他 Citrix Cloud 社区成员也可能提供帮助或加入讨论。

您不需要登录即可阅读论坛主题。但是，必须登录才能发表主题或回复主题。要登录论坛，请使用您的现有 Citrix 帐户凭据，或者使用您在创建 Citrix Cloud 帐户时提供的电子邮件地址和密码。要创建 Citrix 帐户，请转到 创建或申请帐户。

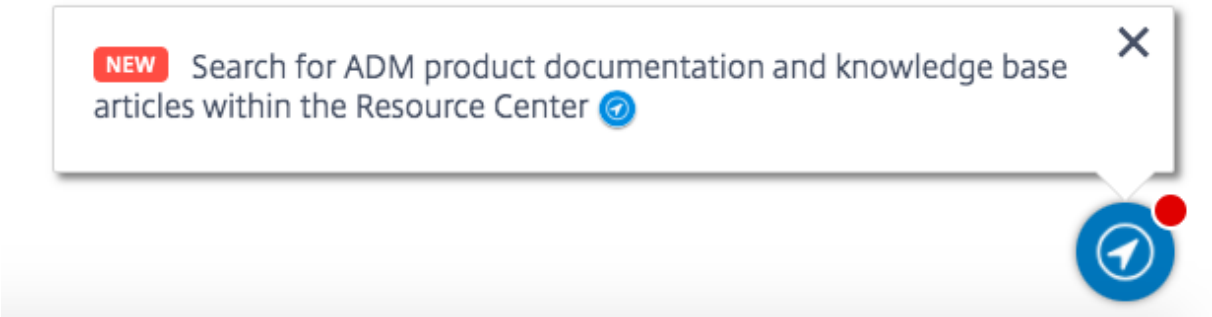
支持文章和文档

NetScaler 提供丰富的产品和支持内容，帮助您充分利用 Citrix Cloud 并解决您在使用 NetScaler 产品时可能遇到的许多问题。

Citrix Cloud 资源中心

Citrix Cloud 资源中心提供多种资源来帮助您开始使用 Citrix Cloud 服务、了解有关功能的更多信息并解决问题。显示的资源适用于您当前正在使用的 Citrix Cloud 中的功能或服务。例如，如果您在 Virtual Apps and Desktops 服务管理控制台中，资源中心会向您显示以下资源。

单击 Citrix Cloud 控制台右下角的蓝色罗盘图标，随时访问资源中心。



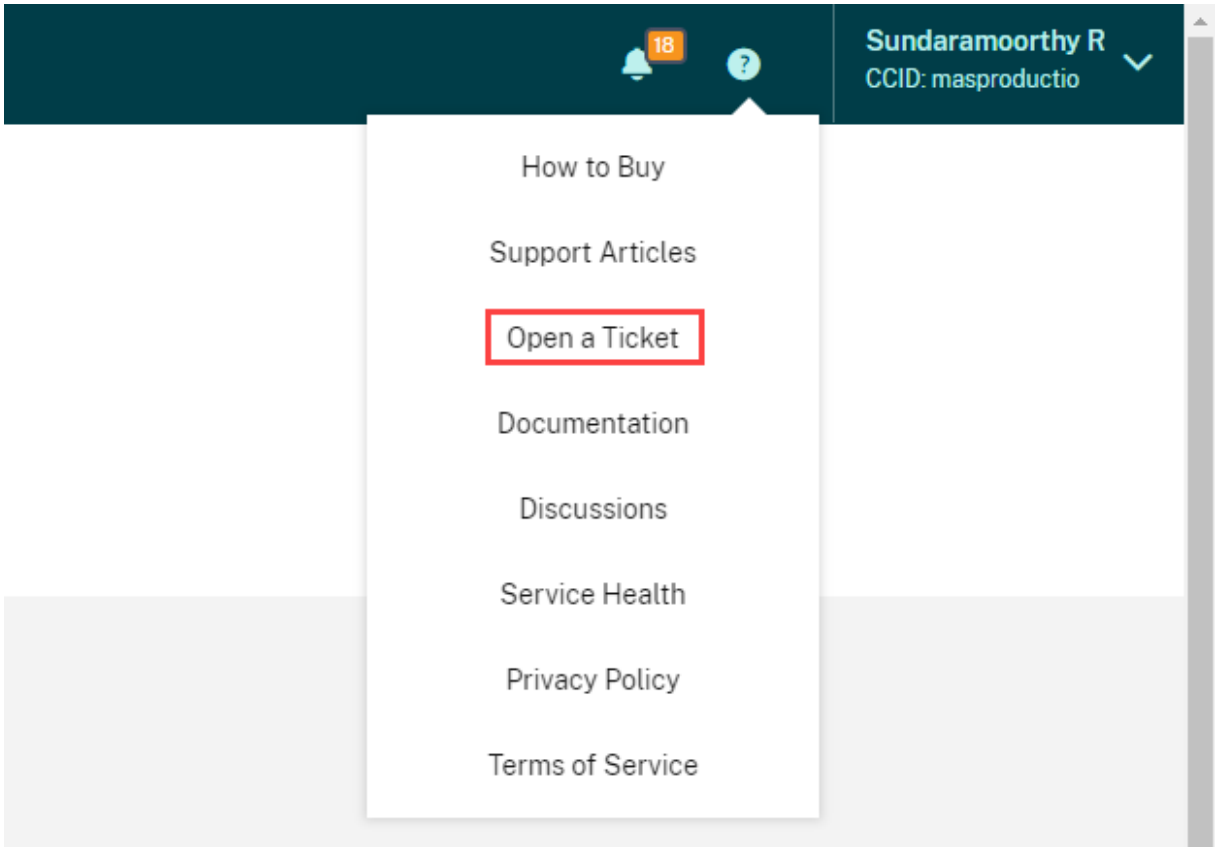
- 入门：提供特定于您当前使用的服务的关键任务的简短指导演练。您还可以找到培训和入门资源链接，以帮助您了解有关服务功能的更多信息并为最终用户做好成功准备。
- 公告：提供有关新发布功能的通知以及指向基本 Citrix 通信的链接。单击功能通知可获得该功能的简短引导式演示。
- 搜索文章：提供常见任务的产品文档和知识中心文章列表，帮助您在不离开 Citrix Cloud 的情况下查找更多文章。在“我该怎么做…”中输入搜索查询 框中显示根据您正在使用的服务筛选的文章列表。一般来说，支持文章首先出现在列表中，其次是产品文档文章。

Citrix Tech Zone

Citrix Tech Zone 包含大量信息，可帮助您了解有关 Citrix Cloud 和其他 NetScaler 产品的更多信息。在这里，您可以找到参考架构、图表、视频和技术论文，它们为设计、构建和部署 Citrix 技术提供了见解。

技术支持

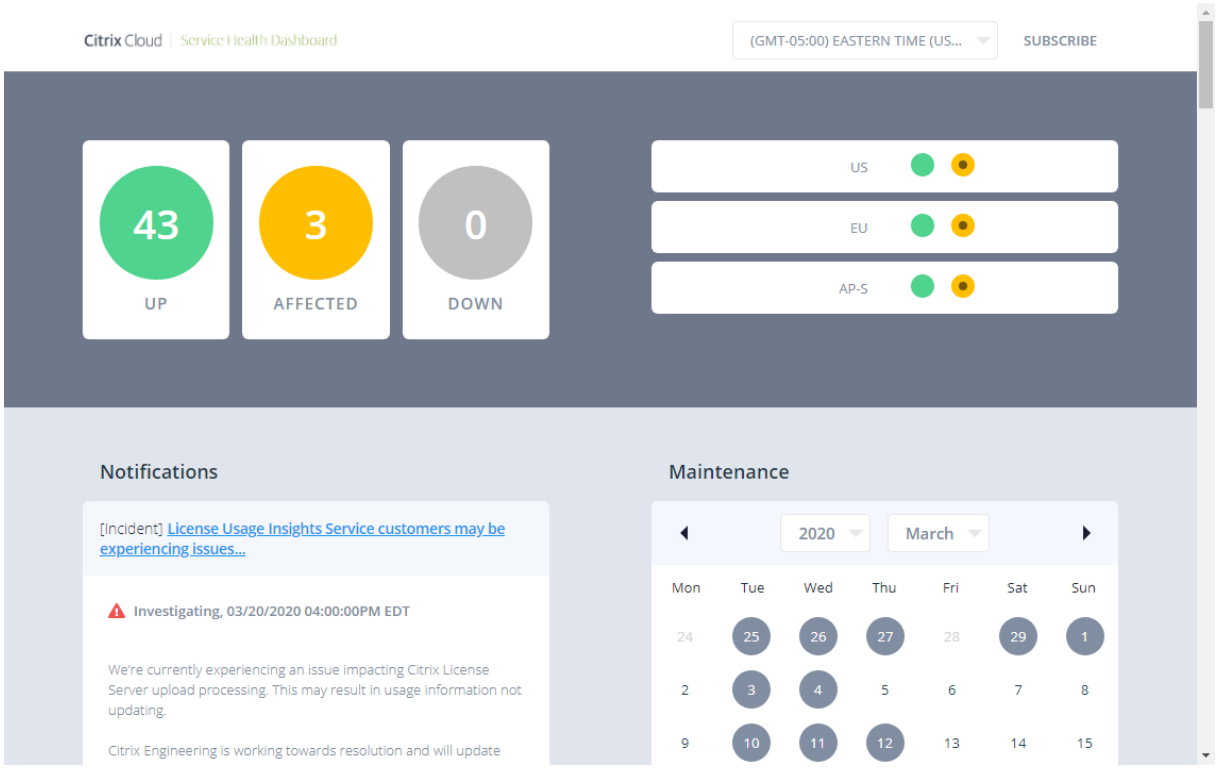
如果您遇到需要技术帮助的问题，请单击屏幕右上角附近的“反馈和支持”图标，然后选择“打开问题单”。



单击“转到我的支持”，然后单击“我的支持”，通过“我的支持”门户打开票证。您还可以使用“我的支持”门户来跟踪您的现有票证并查看您当前的产品权利。

服务运行状况控制板

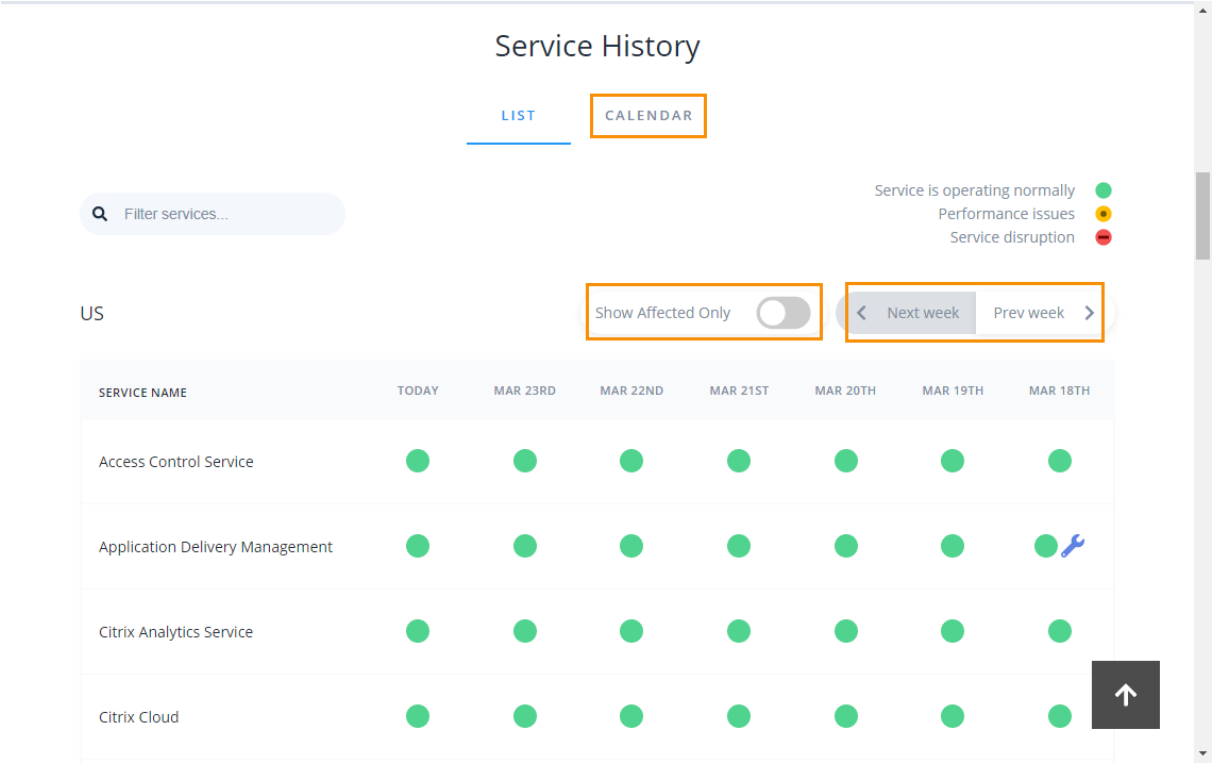
Citrix Cloud 服务运行状况控制面板 概述了每个地理区域 Citrix Cloud 平台和服务的实时可用性。如果您在使用 Citrix Cloud 时遇到任何问题，请检查服务运行状况控制面板，以验证 Citrix Cloud 或特定服务是否正常运行。



使用控制面板了解有关以下条件的更多信息：

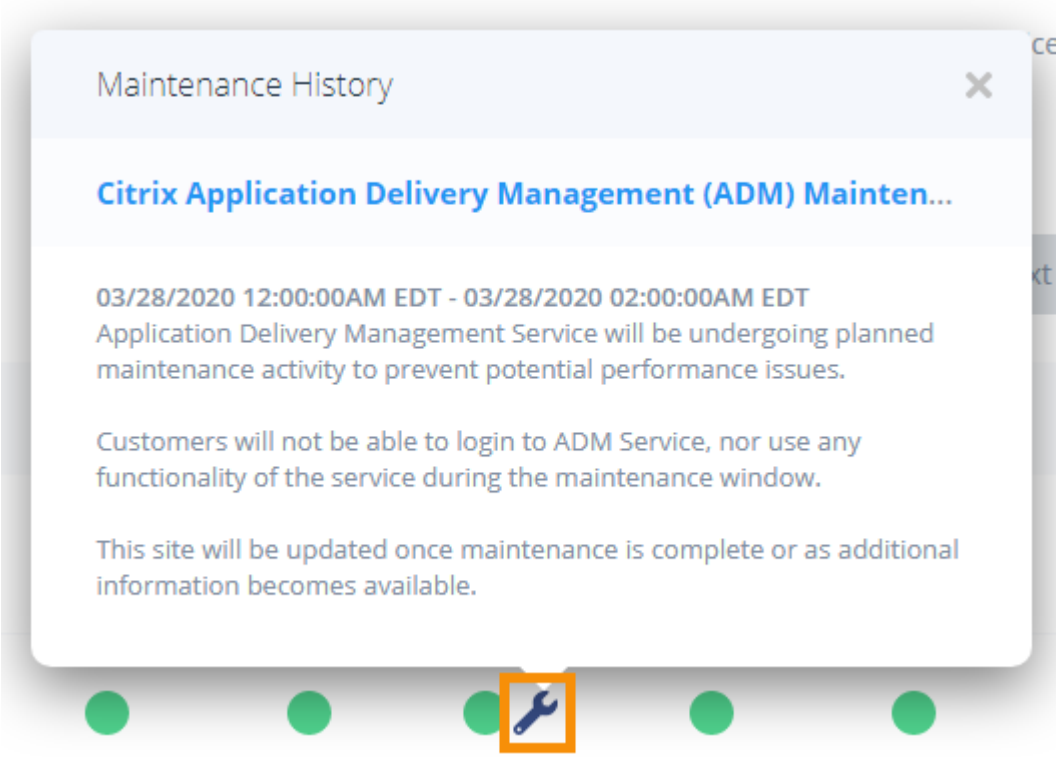
- 所有 Citrix Cloud 服务的当前可用性状态，按地理区域分组
- 过去七天（默认）或之前七天增量的每项服务的服务运行状况历史记录
- 特定服务的维护窗口

默认情况下，服务运行状况以列表形式显示，但您也可以在日历视图中显示状态。选择“下一步”或“上一 步”以七天为间隔滚动浏览服务运行状况历史记录。您也可以筛选列表以仅显示受影响的服务。

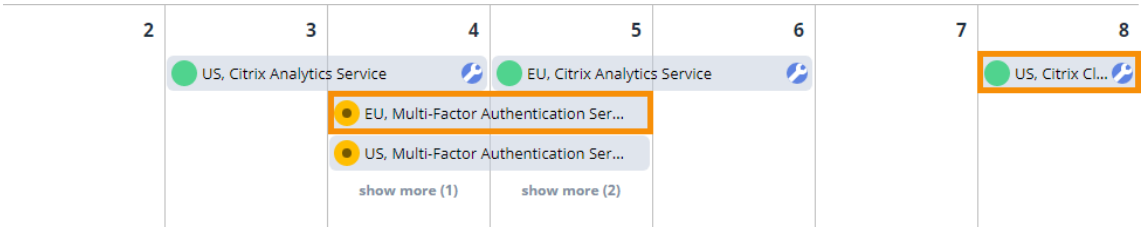


要查看有关受影响服务的服务运行状况事件的更多详细信息，请执行以下操作：

- 在列表视图中，单击服务指示器旁边的图标以查看有关服务运行状况事件的更多详细信息。

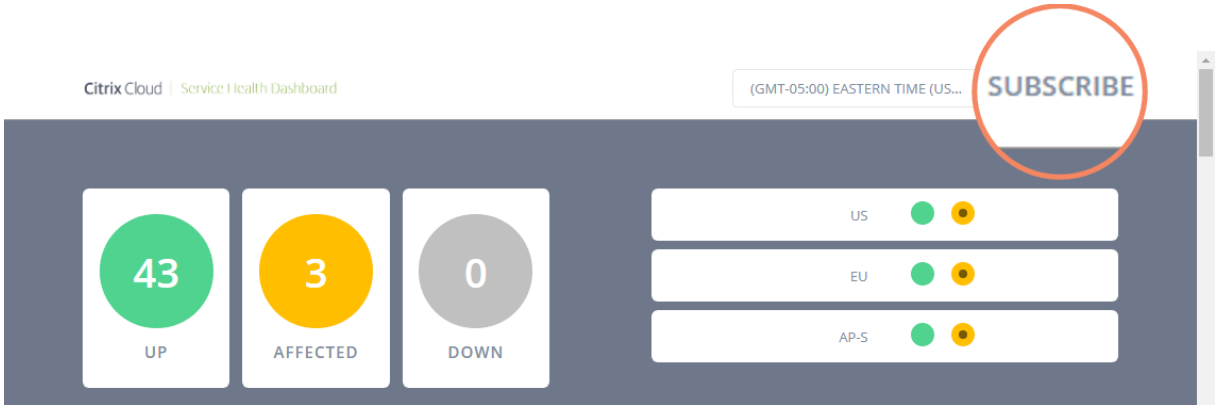


- 在日历视图中，单击服务条目以查看服务运行状况事件的状态。

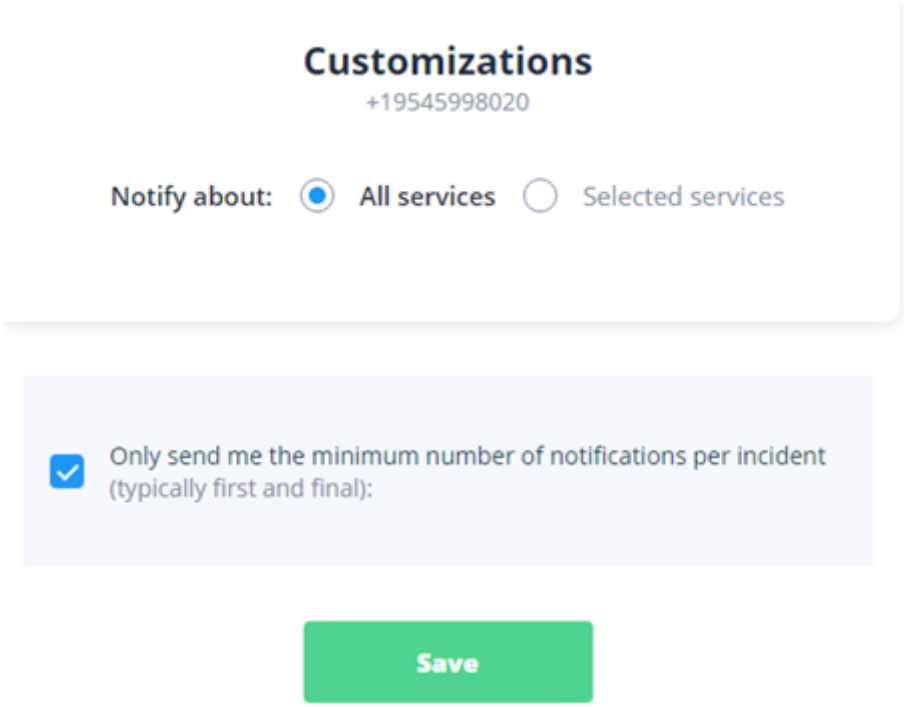


服务运行状况订阅

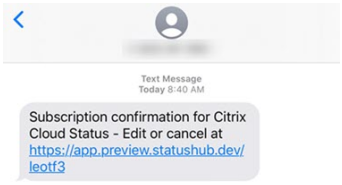
要接收服务运行状况通知，请单击控制面板右上角的“订阅”，然后选择要使用的通知方法。

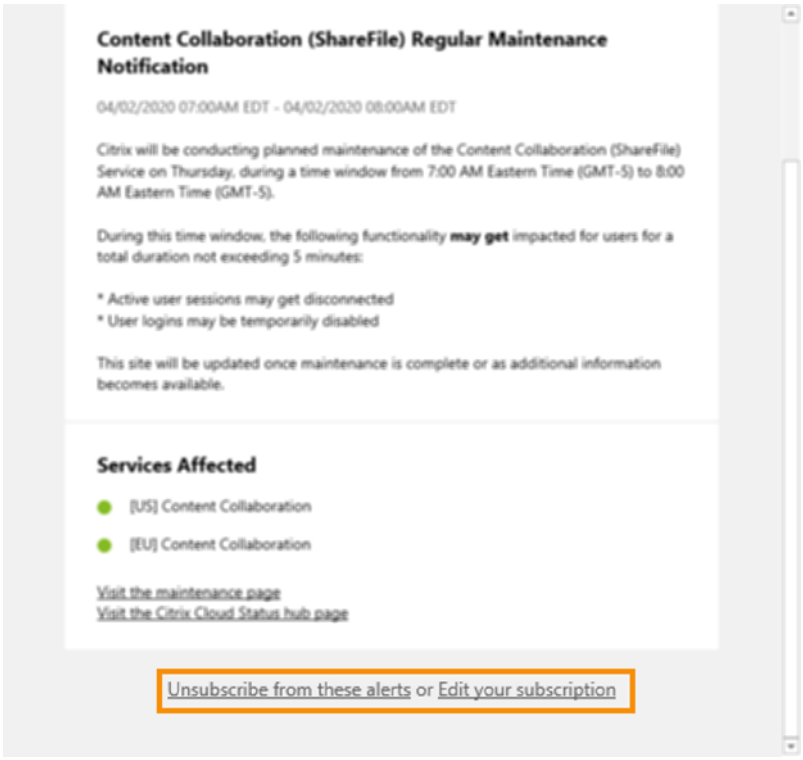


您可以订阅所有服务的通知，也可以只订阅所选服务的通知。默认情况下，您会收到有关服务运行状况事件的所有通知。要限制事件期间的通知频率，您可以选择仅接收第一条和最后一条通知。



根据订阅方法，取消订阅和更改首选项的链接包含在您收到的订阅确认消息（例如，订阅电话通知时）或每条通知消息（例如，订阅电子邮件通知时）中。





要取消订阅或更改您的订阅偏好，请执行以下操作：

1. 找到现有通知并选择链接以取消订阅或更改您的通知首选项。
2. 如果取消订阅，请选择“取消订阅”，然后选择要取消的通知方法。要使用所有通知方式进行订阅，请选择“删除所有订阅”。
3. 如果更改首选项，请选择通知方法，对服务和最小事件通知进行相应更改，然后选择“保存”。

使用 **Console Advisory Connect** 低接触加载 **NetScaler** 实例

April 10, 2024

随着混合多云 (HMC) 基础架构的发展，管理、监视、分析和故障排除 NetScaler 实例面临多重挑战。集中式控制器提供对完整基础结构以及在其上运行的所有应用程序的可见性，成为一个小时的需要。

在当今世界中，需要以快速、简单和低接触的方式将您的实例加载到中央控制器。考虑到这一需求，NetScaler 控制台启动了新的入职流程，使您可以更快地全面了解 HMC 部署。

概述：**NetScaler** 控制台入门流程的组件

该工作流程的组成部分是两个 ADC 端组件：NetScaler 服务连接和 Call Home。

- 控制台公告连接：这是 NetScaler 中的一项新功能，有助于实现 NetScaler 实例无缝加载到 NetScaler 控制台上。此功能允许 NetScaler 实例自动连接到 NetScaler 控制台，并将系统、使用情况和遥测数据发送到 NetScaler 控制台。基于这些数据，NetScaler 控制台为您提供有关 NetScaler 基础架构的见解和建议。例如快速识别性能问题、高资源使用率和严重错误。

  控制台公告连接适用于以下 NetScaler 版本：

  - NetScaler MPX 和 VPX 映像版本 12.1 57.18 及更高版本以及 13.0 61.48 及更高版本。有关更多信息，请参见适用于 NetScaler 设备的 NetScaler 控制台连接简介。
  - NetScaler SDX 版本映像 12.1 58.14 及更高版本以及 13.0 61.48 及更高版本。有关更多信息，请参见适用于 NetScaler SDX 设备的 NetScaler 控制台连接简介。

- **Call Home**：这是 ADC 中的一项现有功能，可定期监视实例并自动将数据上载到 Citrix 技术支持服务器。有关更多详情，请参阅“Call Home。Call Home 收集的数据还会传送到 NetScaler 控制台，以启用这一新工作流程。

所有具有互联网连接或 Call Home 连接的 NetScaler 实例，或启用 NetScaler 控制台连接的实例都连接到 NetScaler 控制台。NetScaler 控制台开始通过 Call Home 路由、NetScaler 控制台连接路由或两者兼而有之，从这些 NetScaler 实例收集相关指标。有关更多信息，请参阅 MPX 和 VPX 实例的数据治 理和 SDX 实例的数据治理。

使用这些数据，NetScaler 控制台为每位客户创建了 NetScaler 实例清单（唯一的组织 ID），向您显示了 NetScalerInstances 的综合清单。NetScaler 控制台还使用这些数据来创建有关您的 NetScaler 和网关实例的见解，从而对您的 HMC 部署提供有意义的见解，发现问题并建议缓解问题的措施。在缓解问题之前，必须先将 NetScaler 实例加载到 NetScaler 控制台。

您可以选 中“选择要加载的 **NetScaler** 和网关实例”，然后选择要加载到 NetScaler 控制台的 NetScaler 实例。开始之后，您将被引导至登录流程。

自动入门流程使用控制台公告连接，这使体验变得自动化、无缝且更快。对于不支持控制台公告连接和自动入门的版本上的 NetScaler 实例，NetScaler 控制台提供基于脚本的入门服务，这是一个半自动化的过程。

> 备注
>
> - 自动和基于脚本的入门使用内置代理。但是，此工作流程还允许您灵活地使用外部代理进行登录。如果您想在 NetScaler 控制台中使用池化许可或完整的分析套件，则可以使用基于外部代理的入门服务。或者，如果您想同时使用池许可和完整的分析套件。内置代理仅支持管理和监视。
> - Console Advisory Connect 收集的指标将直接发送到 NetScaler 控制台服务端点。即使 NetScaler

> 是 NetScaler 控制台上托管/发现的 NetScaler，并且已经为该 ADC 配置了外部代理，指标也会直接从 NetScaler 发送到 NetScaler 控制台服务端点，而不是通过外部代理路由。

登录快速浏览

登录旅程中的第一个接触点是产品发起的电子邮件。以下是登录旅程的简要介绍：

1. 一封由 **NetScaler** 产品发起的邮件：您将收到一封来自 NetScaler 控制台的邮件，其中包含有关您的 NetScaler 基础架构的一些重要见解，并邀请您开始使用 NetScaler 控制台。在电子邮件中单击“加入 **ADM** 服务”。将出现 **Citrix Cloud** 页面。
2. 在 **Citrix Cloud** 登录页面中：
   - 如果您是 Citrix Cloud 的现有客户，请使用您的 **Citrix.com**、**My Citrix** 或 **Citrix Cloud** 凭据登录 Citrix Cloud。
   - 如果您不是 Citrix Cloud 的现有客户，请注册 Citrix Cloud。有关更多信息，请参阅 注册 Citrix Cloud。

   > 备注
   >
   > - 如果您是多个组织 ID 的一部分，并且其中一个组织 ID 位于 Citrix Cloud 中，请使用您的现有凭据登录。然后，完成新组织 ID 的登录工作流程。
   > - 您可以启用或禁用在基于 Console Advisory Connect 的低接触入职工作流程中收到的电子邮件通知。有关更多信息，请参阅 电子邮件设置。
3. **NetScaler** 控制台欢迎页面：您可以概述 NetScaler 控制台及其优势。
4. 对您的 **NetScaler** 和网关实例的见解：您可以详细了解整个 NetScaler 基础架构，包括安全公告（有关当前 NetScaler CVE 的建议）、升级公告（基于 EOM/EOL 时间表的建议）、关键指标、趋势，重点介绍影响 NetScaler 性能和运行状况的问题，并推荐缓解问题的方法。
5. 选择要加入的 **NetScaler** 和网关实例：您可以获得 NetScalerInventory 的综合视图。您可以选择要将哪些 NetScaler 实例加载到 NetScaler 控制台。
6. 将 **NetScaler** 实例加载到 **NetScaler** 控制台：根据选择的入门的 NetScaler 实例，NetScaler 控制台会指导您完成入门流程。默认情况下，选择内置代理进行自动加载。
7. **NetScaler** 控制台 **GUI** 控制面板：入门完成后，系统会引导您进入 NetScaler 控制台实例控制面板。

有关每种入门方法的更多详情，请参见 使用 NetScaler 控制台连接加载 NetScaler 实例。

使用控制台公告连接加载 **NetScaler** 实例

April 10, 2024

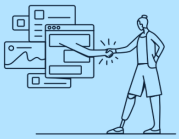
本文档提供分步指南，帮助您开始使用 NetScaler 控制台。在开始之前，请阅读 NetScaler 控制台如何启动新的入门流程，该流程可让您更快地全面了解混合多云 (HMC) 部署。参见使用 NetScaler 控制台连接低接触加载 NetScaler 实例。

步骤 **1**：开始

您将收到一封来自 NetScaler 控制台的电子邮件，其中包含有关您的 NetScaler 基础架构的一些关键见解，并邀请您开始使用 NetScaler 控制台。

citrix

Onboard to Citrix ADM Service for Security Advisory



Hello [redacted] Org ID - [redacted]

As a valued Citrix customer, your application delivery infrastructure security is our top concern. To help keep your infrastructure secure, we just launched **security advisory and upgrade advisory** for your Citrix ADCs.

These new features can identify outdated software deployed in your ADC fleet, notify you of known vulnerabilities in these releases, and suggest steps you can take to remediate these issues.

Below, you'll see a preview of these advisories and other key insights customized to your infrastructure. More information and recommended actions are available when you onboard to Citrix ADM service. You can get started with Citrix ADM Service Express account at no additional cost.

Insights on your ADC & Gateway infrastructure

These insights are based on data provided via Call Home and/or Citrix ADM Service Connect.

ADC instances by platforms

30	20	5	5
Total	VPX	SDX	MPX

Security Advisory

5 ADC instances are on versions with known common vulnerability exposures (CVEs).
This advisory is based on ADC build version scan only & more conclusive & exhaustive security advisory insights can be seen after onboarding all your ADCs to ADM Svc

Upgrade Advisory

2 ADC instances are on versions that have reached end of life in last 365 days or earlier.

1 ADC instance is on a version that will reach end of life in next 365 days.

3 ADC instances are on versions that have reached end of maintenance in last 365 days or earlier.

4 ADC instances are on versions that will reach end of maintenance in next 365 days.

2 ADC instances are on older builds and releases.

Recent events

4 ADC instances encountered SSL card failure.
2 ADC instances encountered hard disk failure.

Resource utilization

2 ADC instances CPU usage exceeded 50%
3 ADC instances memory usage exceeded 50%

ADC deployment

5 ADC instances are not deployed as High Availability (HA) pair. Citrix ADM recommends HA pair for production ADC instances.

To get more details and recommendations on these insights, **onboard your ADC instances to Citrix ADM service, today.**

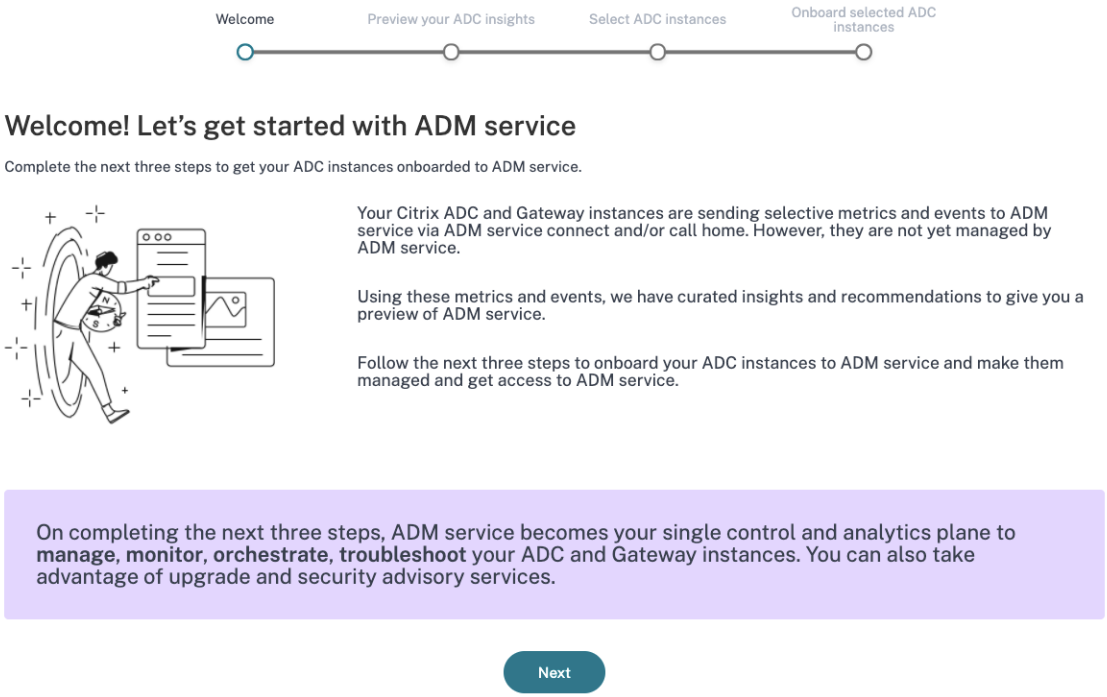
As a first step, you will need to create Citrix Cloud account by clicking on the button below.

Onboard to ADM Service

1. 在电子邮件中，单击“加入 **ADM** 服务”。将出现 **Citrix Cloud** 页面。
2. 在 **Citrix Cloud** 登录页面中：
   - 如果您是 Citrix Cloud 的现有客户，请使用您的 **Citrix.com**、**My Citrix** 或 **Citrix Cloud** 凭据登录 Citrix Cloud。
   - 如果您不是 Citrix Cloud 的现有客户，请注册 Citrix Cloud。有关更多信息，请参阅 注册 Citrix Cloud。

   > 备注
   >
   > - 如果您是多个组织 ID 的一部分，并且其中一个组织 ID 位于 Citrix Cloud 中，请使用您的现有凭据登录。然后，完成新组织 ID 的登录工作流程。
   > - 您可以启用或禁用在基于 Consolve Advisory Connect 的低接触入职工作流程中收到的电子邮件通知。有关更多信息，请参阅 电子邮件设置。

3. 在 NetScaler 控制台登录页面上，花点时间阅读您的存在原因以及使用 NetScaler 控制台的好处。



> 注意
>
> 邮件中的安全公告见解仅基于 NetScaler 构建版本扫描。在将 NetScaler 实例加入 NetScaler 控制台后，您可以看到更具决定性和详尽的安全公告见解。

1. 单击下一步。“关于您的 **NetScaler** 和网关实例的见解”页面将打开。

接下来的几个步骤将作为指导性工作流程，让您预览 NetScaler 控制台可以提供的功能，并帮助您无缝地将 NetScaler 实例加载到 NetScaler 控制台上。

第 2 步：深入了解您的 NetScaler 和 Gateway 实例

此见解页面使用通过 Call Home 或 NetScaler 控制台连接或同时通过 Call Home 和 NetScaler 控制台连接收集的数据，提供有关您的 NetScaler 实例的见解。本页让您深入了解整个 NetScaler 基础架构，包括安全公告（有关当前 NetScaler CVE 的建议）、升级公告（基于 EOM/EOL 时间表的建议）、关键指标、趋势，重点介绍了影响 NetScaler 性能和运行状况的问题，并推荐了缓解问题的方法。这些见解和建议只是对 NetScaler 控制台提供的众多优势和增值的一小部分预览。为了获得更多好处、详细见解并能够运行建议的操作，您必须将 NetScaler 实例载入 NetScaler 控制台。

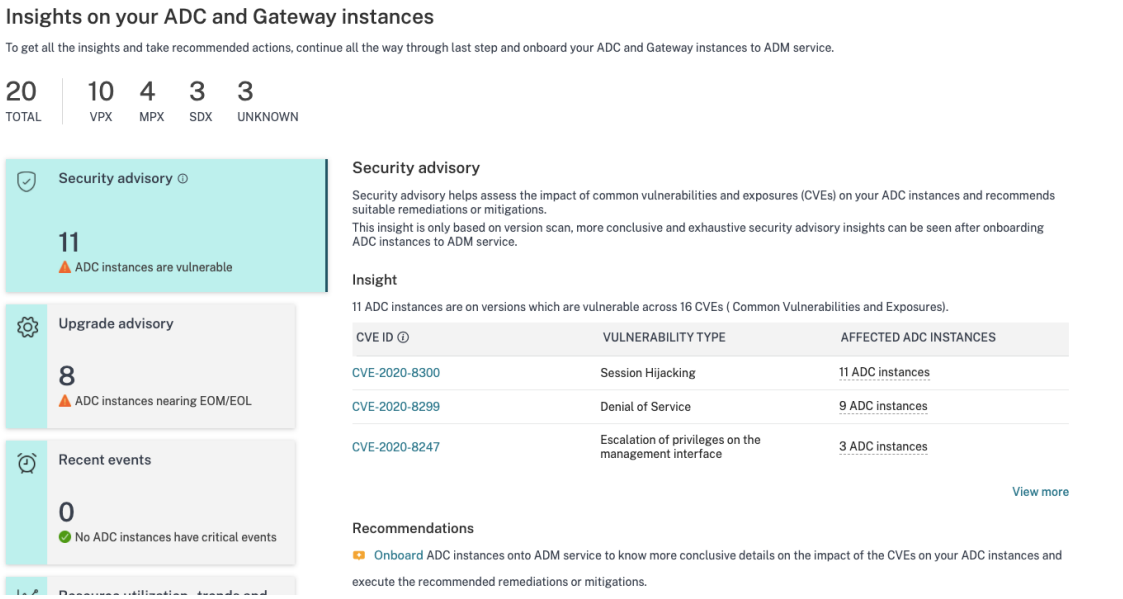
洞察和建议分为以下类型：

- 安全警告：加 载 NetScaler 实例以获取对您的 NetScaler 实例的 CVE 影响详情，并运行建议的补救措施或缓解措施。
- 升级建议：将 NetScaler 实例载入 NetScaler 控制台，然后升级已达到或即将达到 EOM/EOL 或处于较旧版本/版本的 NetScaler 实例。
- 最近发生的事件：将 NetScaler 实例 加载到 NetScaler 控制台以定期监视 200 多个事件，并制定规则以通过电子邮件、PagerDuty、Slack、ServiceNow 获得通知，采取适当的措施。
- 资源利用率——趋势和异常：将 NetScaler 实例加载到 NetScaler 控制台，以全面了解 NetScaler 实例运行状况、性能问题以及缓解这些问题的建议。您还可以评估 NetScaler 实例的预测的 CPU 和内存使用情况。
- **NetScaler** 部署指南：在 NetScaler 控制台上使用配置作业，将 NetScaler 实例加载到 NetScaler 控制台并将其配置为 HA 对。

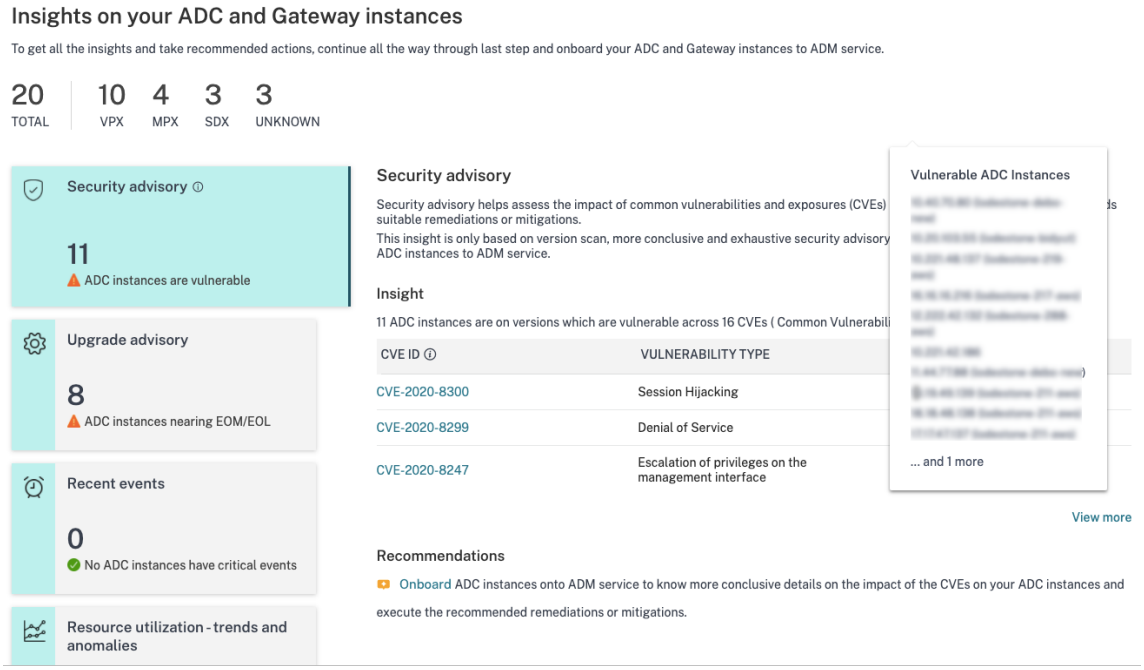
1. 安全公告：NetScaler 控制台安全公告会提醒您有关可能使 NetScaler 实例面临风险的漏洞，并建议缓解措施和补救措施。

   > 注意：
   >
   > 入门邮件和指导性工作流程中的安全公告见解仅基于 NetScaler 构建版本扫描。将您的 NetScaler 实例加载到 NetScaler 控制台后，您可以看到确凿而详尽的安全公告见解 示例：如果 CVE 需要版本扫描和配置扫描以进行漏洞评估，则入门邮件和指导性工作流程会根据版本扫描显示结果。因此，可能会有误报。要了解对影响的更确切、更准确的评估，请将 NetScaler 加入 NetScaler 控制台。上线后，NetScaler 控制台安全公告根据版本扫描和配置扫描显示了影响评估，该评估易受攻击的 NetScaler 评估。

   您可以检查 CVE ID、漏洞类型和受影响的 NetScaler 实例。CVE ID 链接会转到安全公告文章。



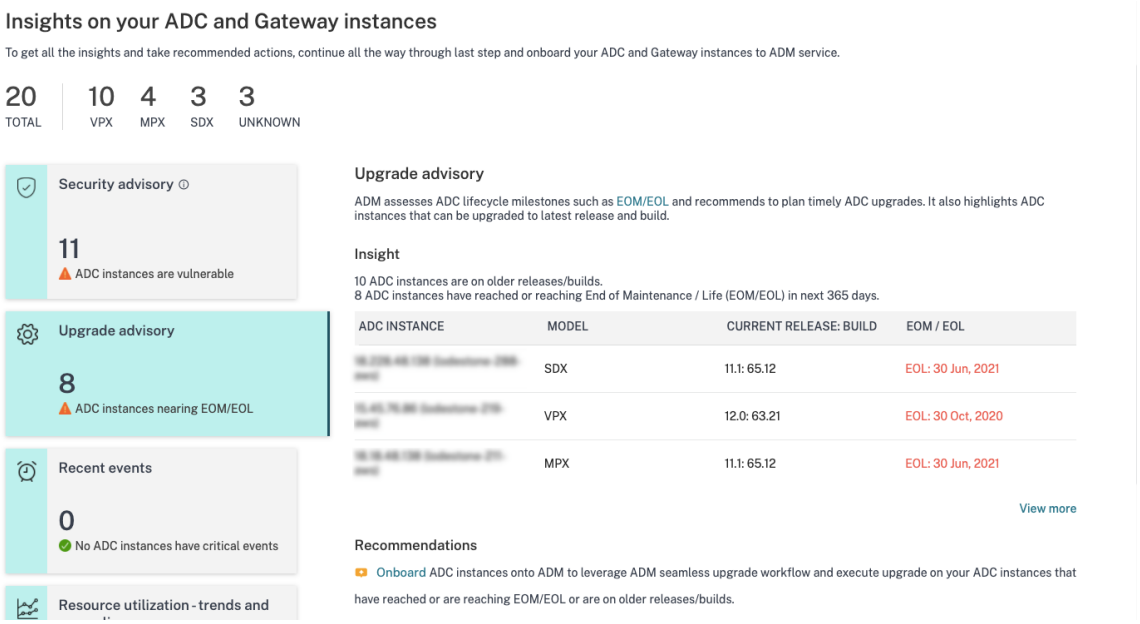
该建议指导您将 NetScaler 实例载入 NetScaler 控制台，以获取 CVE 对您的 NetScaler 实例影响的更多详细信息，并运行建议的缓解措施或补救措施。单击受影响的 NetScaler 实例以查看受影响实例的 IP 地址。



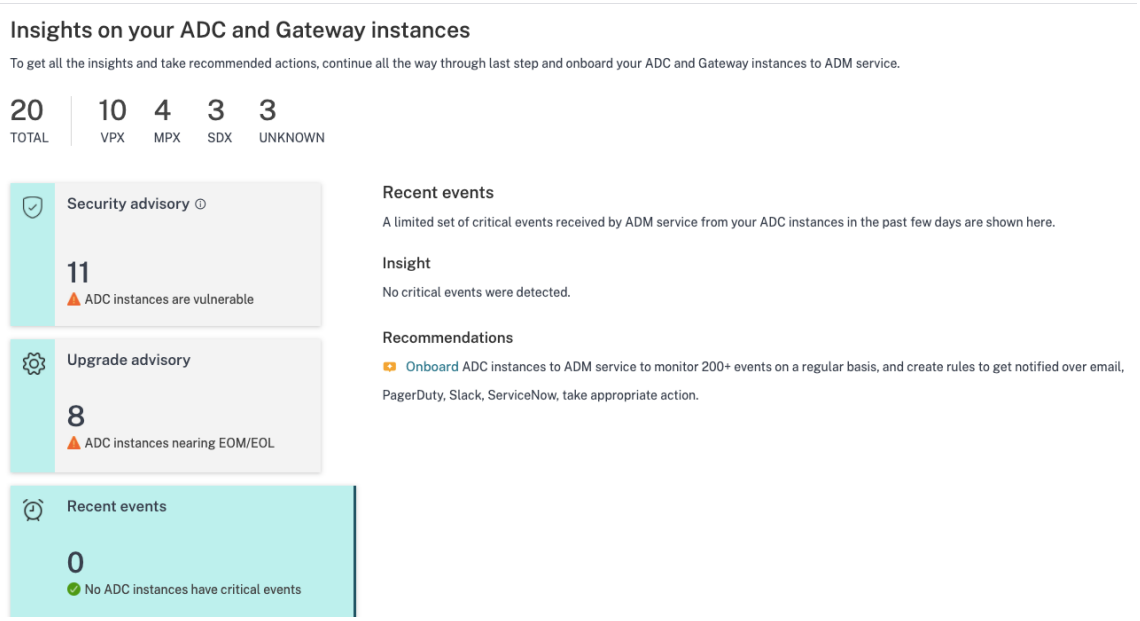
2. 升级建议：使用此公告来检查哪些 NetScaler 实例接近 EOM/EOL 或处于较旧版本中。

   基于这些见解，NetScaler 控制台建议您在 EOM/EOL 之前计划及时升级，或者从最新功能和修复中受益。

   要执行升级，必须将您的 NetScaler 实例加载到 NetScaler 控制台上。

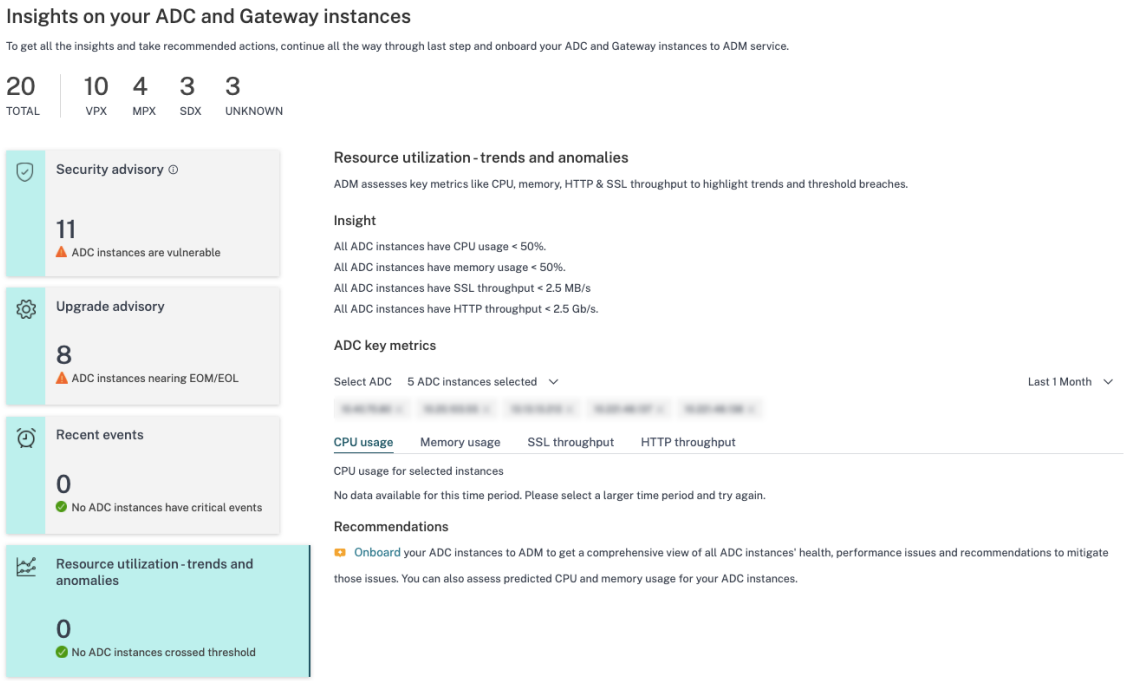


3. 近期事件：获取在 NetScaler 实例上发生的一些严重错误的详细信息以及发生错误的 NetScaler 实例的列表。

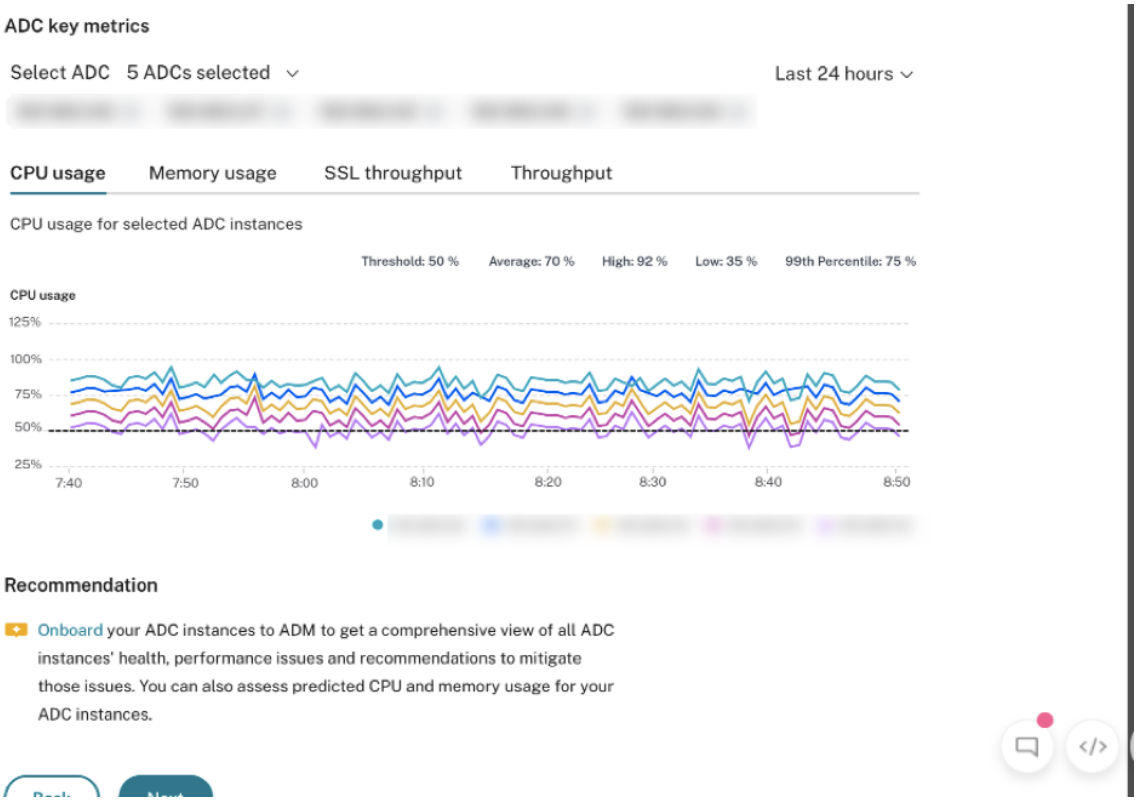


4. 资源利用率-趋势和异常：查找有关 CPU、内存、HTTP 吞吐量和 SSL 吞吐量高资源利用率的见解。对于每项见解，NetScaler 控制台都会提出建议的操作建议。为了更深入地了解这些见解和建议，您必须将您的 NetScaler 实例载入 NetScaler 控制台。登录后的一些好处是：

   - CPU：在 NetScaler 控制台上预测未来 24 小时的 CPU 使用率。
   - 内存：在 NetScaler 控制台上预测未来 24 小时的内存使用情况。
   - SSL 吞吐量：在 NetScaler 控制台上使用智能应用分析查看 SSL 实时优化。
   - HTTP 吞吐量：使用基础架构分析解决 NetScaler 吞吐容量问题。

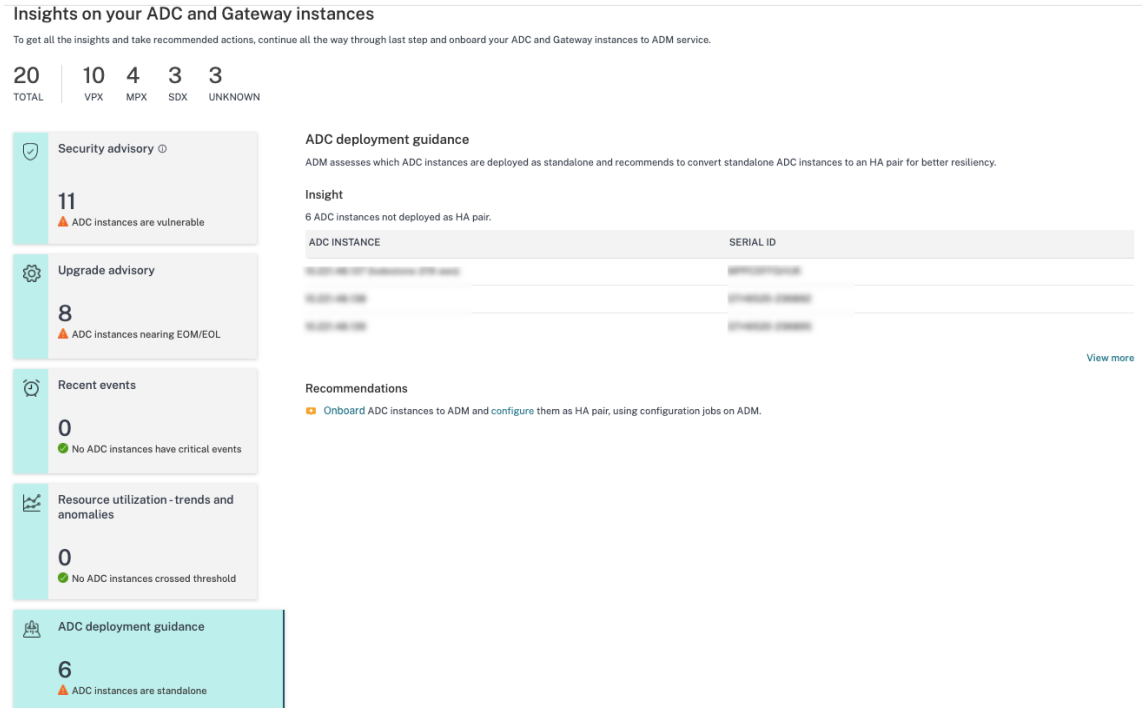


- 关键指标：获取与 CPU、内存、HTTP 吞吐量、SSL 吞吐量相关的关键指标的详细信息，并发现指标中的异常趋势。



5. 部署指南：了解作为独立的 NetScaler 部署的 NetScaler 实例。NetScaler 控制台建议将这些 NetScaler 实例配置为 HA 对，以提高灵活性。这要求您将 NetScaler 实例加载到 NetScaler 控制台，然后使用维护任务将

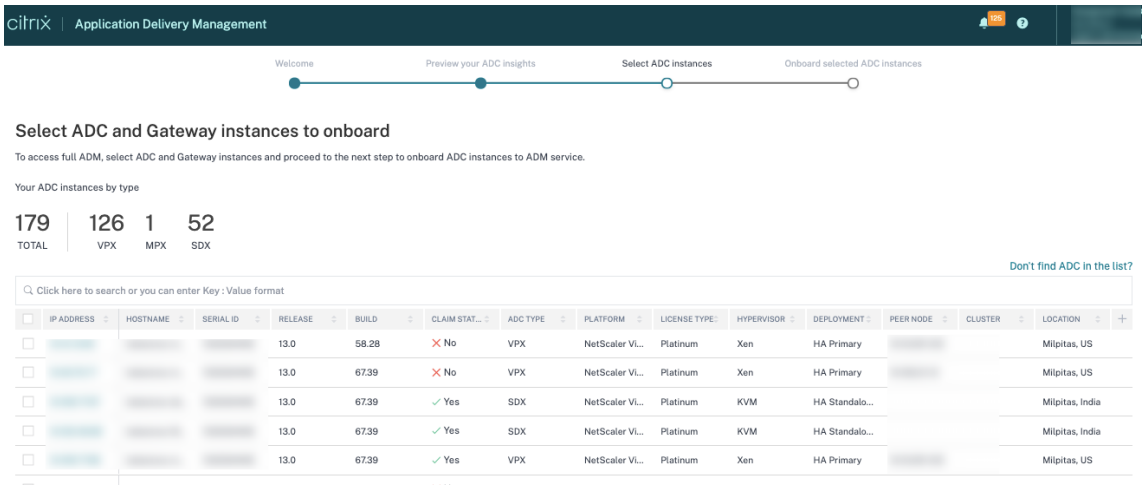
实例配置为 HA 对。



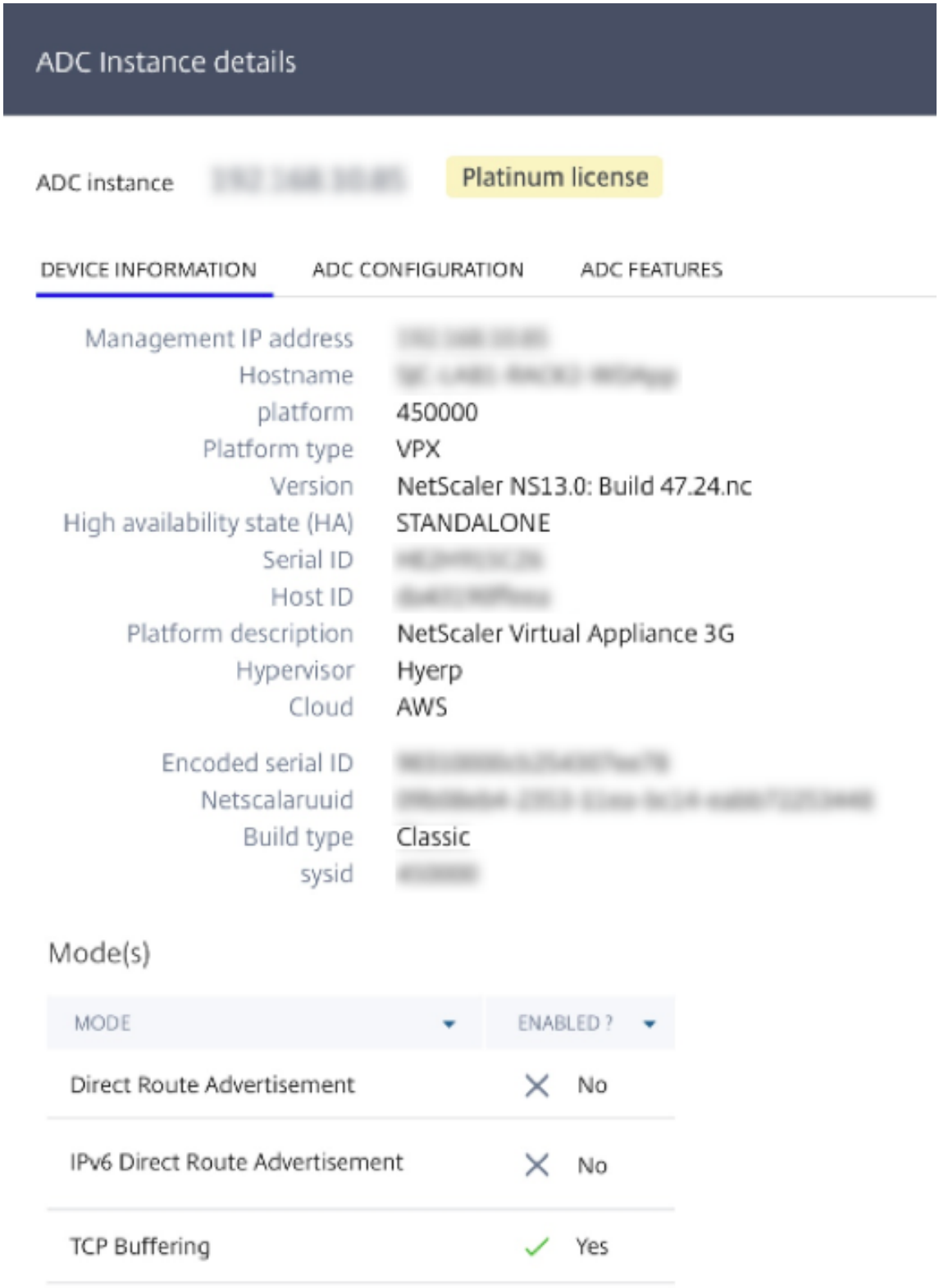
第 **3** 步：选择要加入的 **NetScaler** 和网关实例

此页面显示您的环境中的所有 NetScaler 和网关实例。查看并选择要加载到 NetScaler 控制台的 NetScaler 和网关实例，然后单击“下一步”。

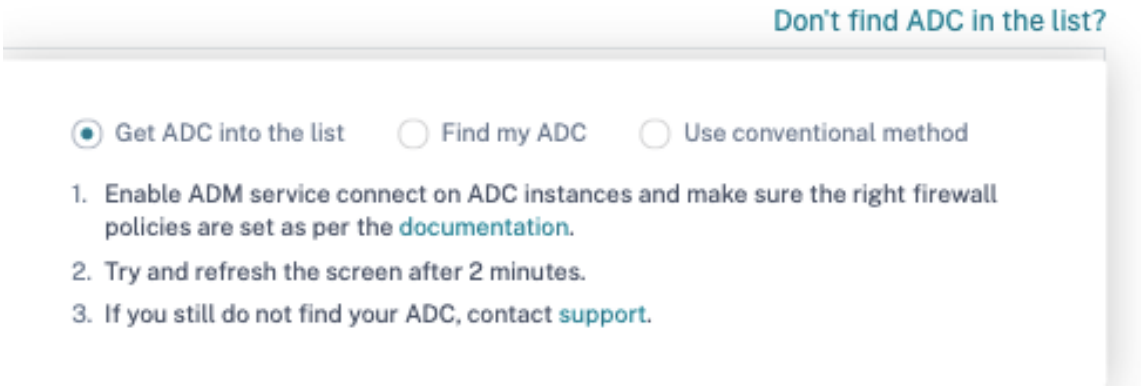
1. 查看并选择要加载到 NetScaler 控制台的 NetScaler 实例。



如果您需要有关任何实例的详细信息，例如设备信息、NetScaler 配置、可用的 NetScaler 功能或许可信息，请单击 NetScaler 实例下的实例 IP 地址。

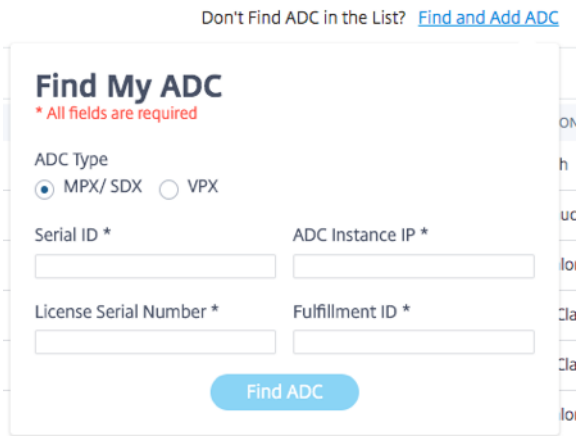


如果您的实例未列出，请使用右上 角列表中的“找不到 **NetScaler**”。



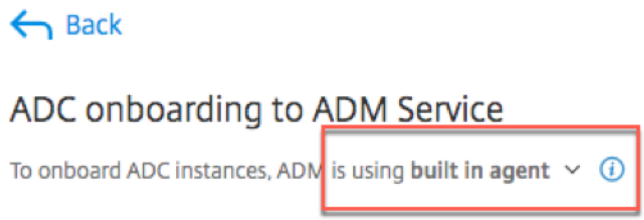
您可以通过三种方式进行操作：按照“将 **NetScaler** 添加到列表”下给出的步骤进行操作，或者使用“查找我的 **NetScaler**”选项。如果这两个步骤无济于事，请单击“使 用传统方法”选项，这将跳过工作流程，引导您了解加载 NetScaler 实例的传统方式。

在“查找我的 **NetScaler**”选项中，在必填字段（序列号、NetScaler 实例 IP 地址、许可序列号和配送 ID）中输入详细信息并进行搜索。



第 **4** 步：将 **NetScaler** 实例加载到 **NetScaler** 控制台

您可以使用内置代理（默认选项）或外部代理来加载实例。



使用内置代理加载 **NetScaler** 实例

自动和基于脚本的入门使用默认设置的内置代理。

自动启动：仅以下 NetScaler 版本支持自动启动：

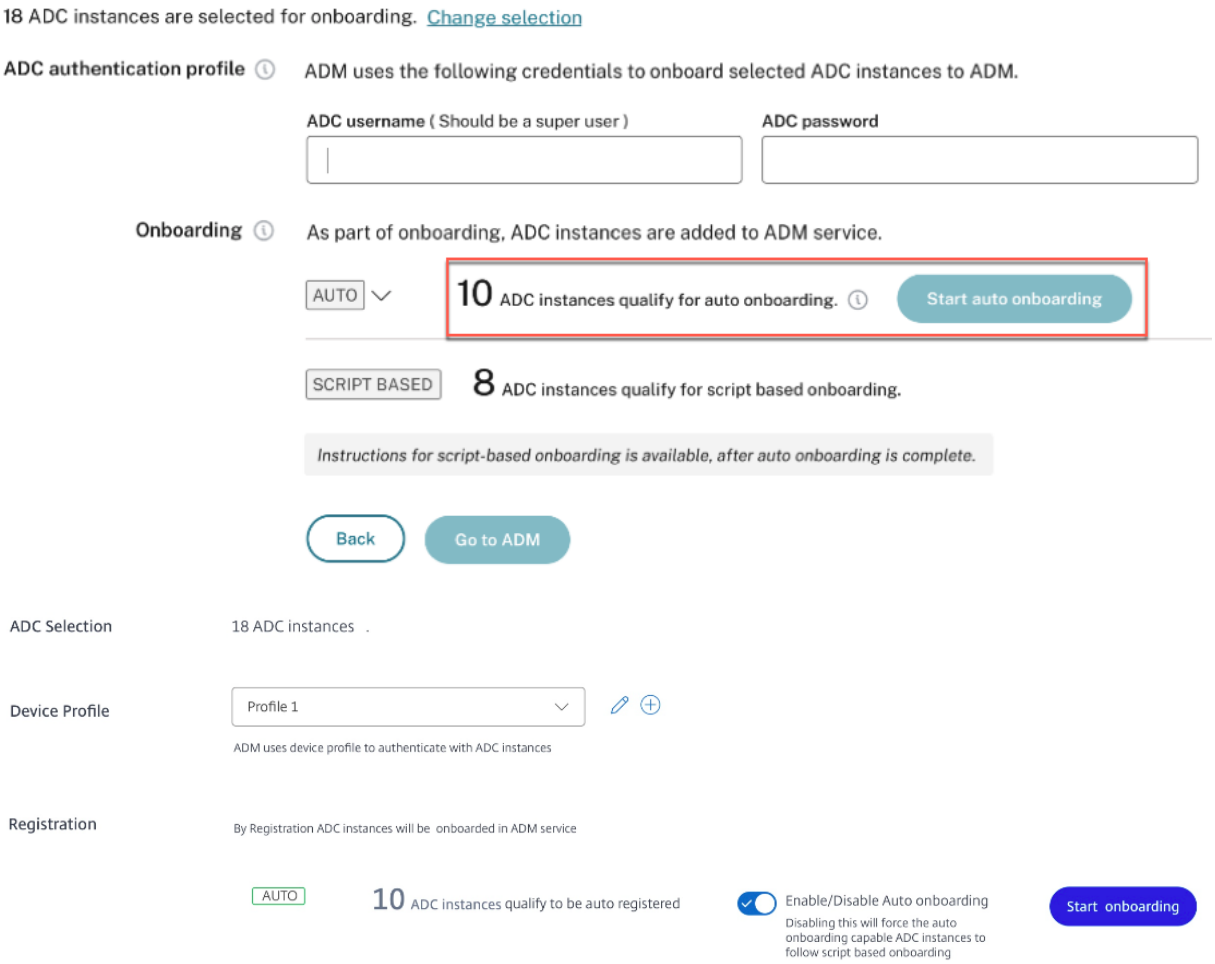
- NetScaler MPX 和 VPX 映像版本 12.1 57.18 及更高版本以及 13.0 61.48 及更高版本
- SDX 版本图像 13.0 61.48 及更高版本和 12.1 58.14 及更高版本

要选择不同的 NetScaler 实例，请单击“更改选择”。

在选定的 NetScaler 实例总数中，某些实例可能符合自动启动条件（基于最低版本标准）。您可以看到符合自动入门条件的实例。

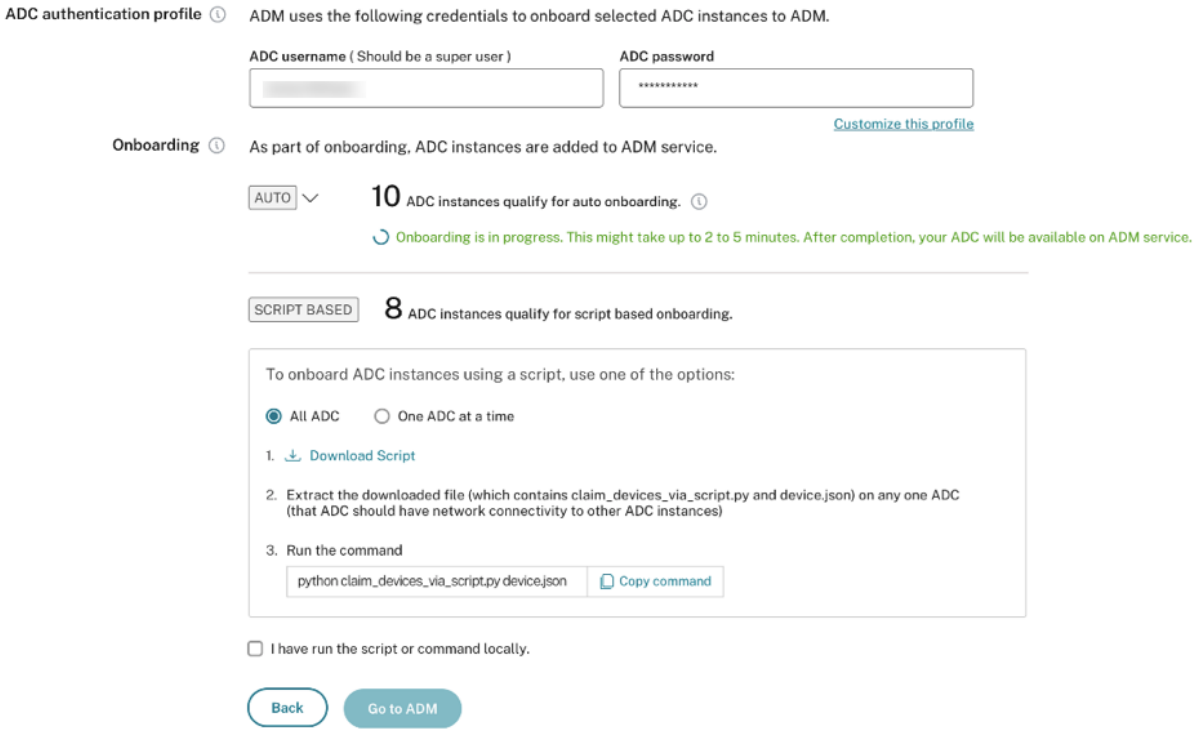
您可以执行载入测试运行，以确保 NetScaler 实例已准备就绪，可以加载。单击“测试”开始测试运行。有关更多信息，请参见 测试 NetScaler 实例的入门准备情况。

如果您想在不运行测试的情况下上线，请输入 NetScaler 用户名和密码。这些凭据必须是 NetScaler 用户管理凭据，NetScaler 控制台使用这些凭据来加载 NetScaler。单击“开始自动加载”，在 NetScaler 控制台上加载您的 NetScaler 实例。



> 注
>
> 意指定 NetScaler 凭据并创建设备配置文件后，ADM GUI 不会再次提示每个 NetScaler 实例输入用户名和密码。但是，您可以从 设备配置文件下拉列表中选择配置文件 来对 NetScaler 实例进行身份验证。

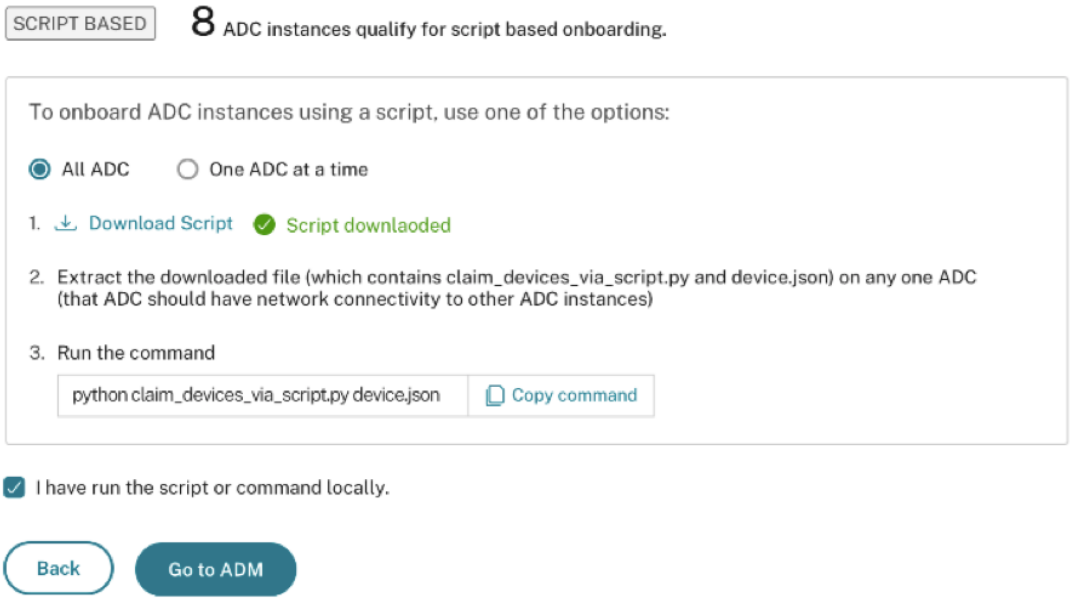
自动入门可能需要 2-5 分钟才能完成。



> 注意：
>
> 如果您不希望 NetScaler 实例自动加载到 NetScaler 控制台，则可以禁用自动载入并使用基于脚本的选项进行入门。

基于脚本的入门：在自动入门完成后，您可以使用基于脚本的入门方式加入其余实例。使用以下选项之一：

- 选项 **1**：下载脚本，提取 tar 文件，然后使用用户界面上给出的命令在任一 NetScaler 实例上运行它。确保运行此脚本的 NetScaler 实例与所有其他选定的 NetScaler 实例具有网络连接。
- 选项 **2**：登录到每个 NetScaler 实例的 CLI 控制台并运行用户界面上给出的命令。有关更多详细信息，请参阅“配置 NetScaler 内置代理以管理实例”文档中的步骤 7。确保为每个 NetScaler 实例生成新的唯一激活码。

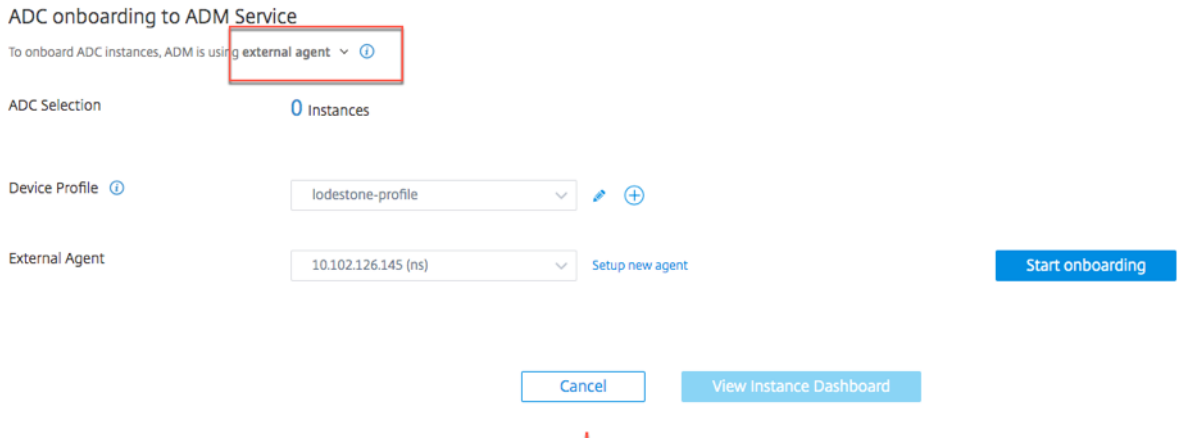


载入所有实例后，单击“转到 NetScaler 控制台”，转到 **NetScaler** 控制台实例管理用户界面控制面板并探索不同的功能。

> 注意：如
>
> 果您是没有 NetScaler 控制台许可的 NetScaler 控制台的新客户，则默认情况下，您的 Citrix 服务帐户为 Express 帐户。有关 NetScaler 控制台帐户权限的更多信息，请参见 使用 Express 帐户管理 NetScaler 控制台资源。

使用外部代理加载 **NetScaler** 实例

如果您想在 NetScaler 控制台中使用池化许可或完整的分析套件，或者两者都使用池化许可和完整的分析套件，则可以使用基于外部代理的入职培训。



完成以下步骤：

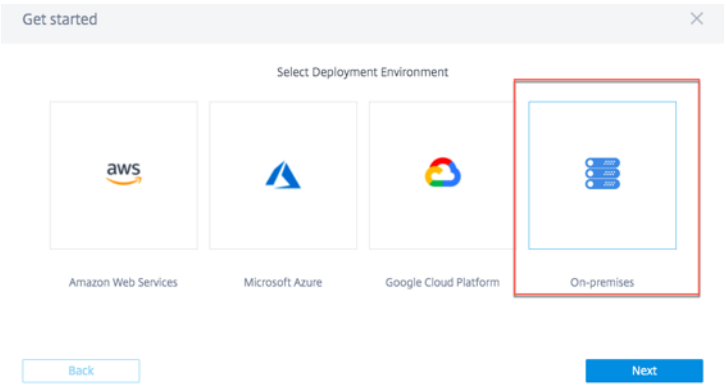
1. 选择设备配置文件。

> 注
>
> 意出于安全原因，您不能使用默认 NetScaler 证书（nsroot/nsroot）进行入门。

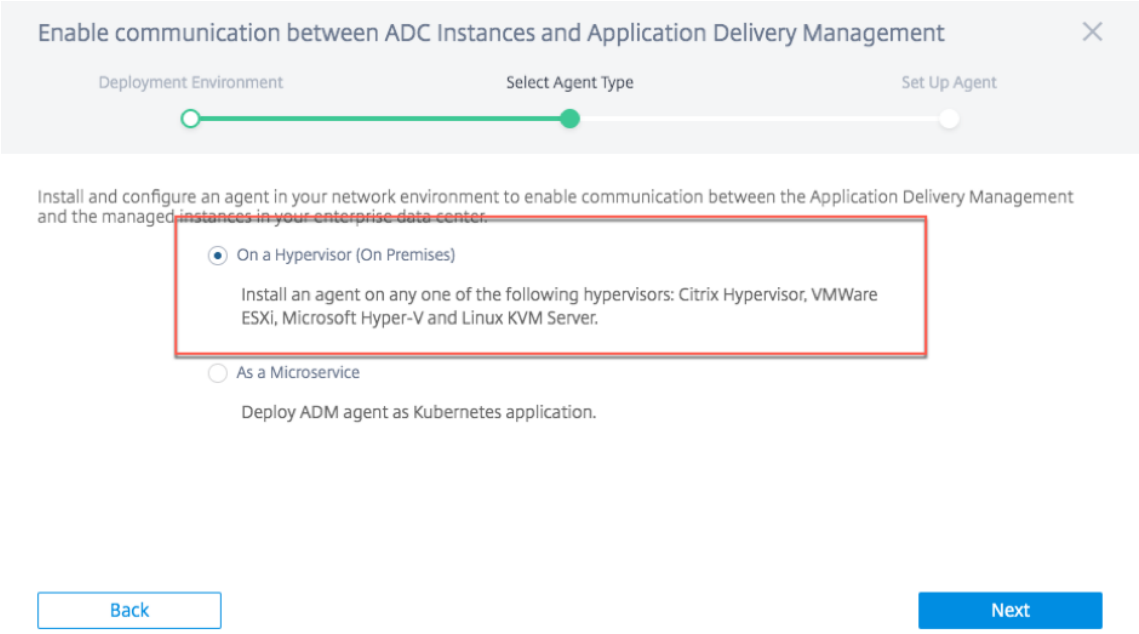
2. 选择外部代理，然后单击 设置新代理。
3. 选择以下任一环境：

   - Amazon Web Services
   - Microsoft Azure
   - Google 云端平台
   - 本地

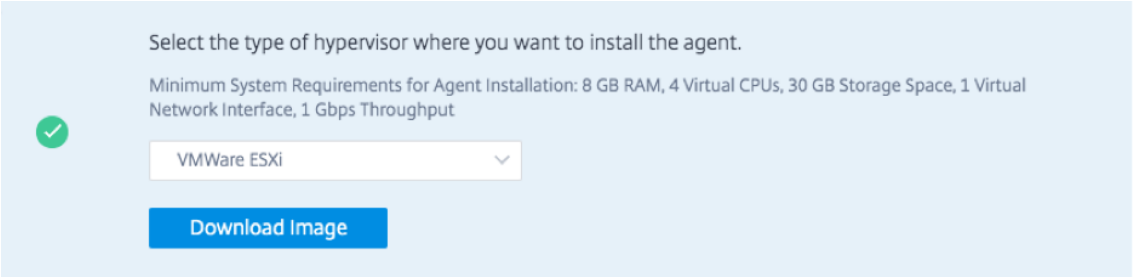
在本地虚拟机管理程序上安装代理　如果选择 本地，则可以在以下虚拟机管理程序上安装代理：Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V、Linux KVM 服务器。



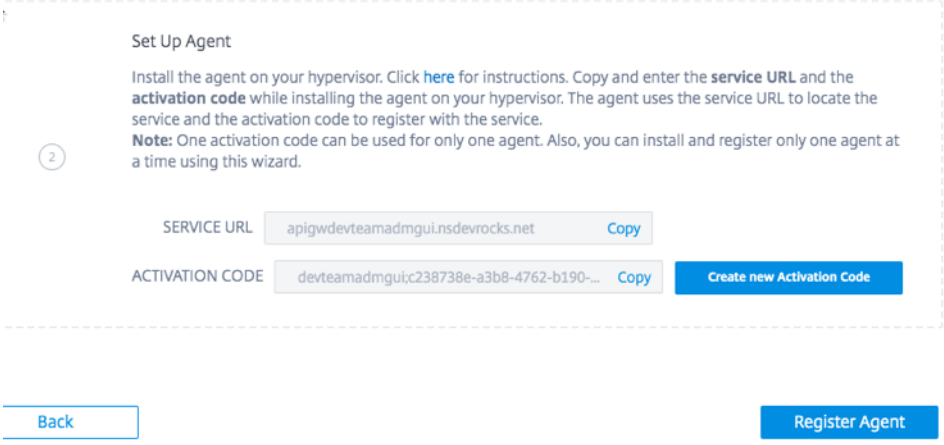
1. 选择 虚拟机管理程序（本地），然后单击 下一步。



2. 选择虚拟机管理程序类型并下载映像，例如 VMware ESXi。

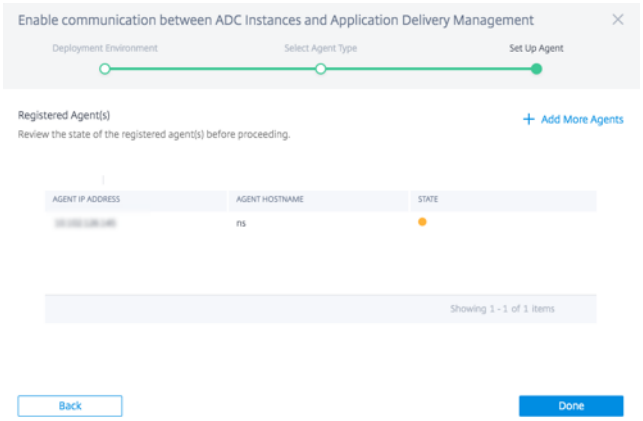


3. 使用服务 URL 和激活码来配置代理。

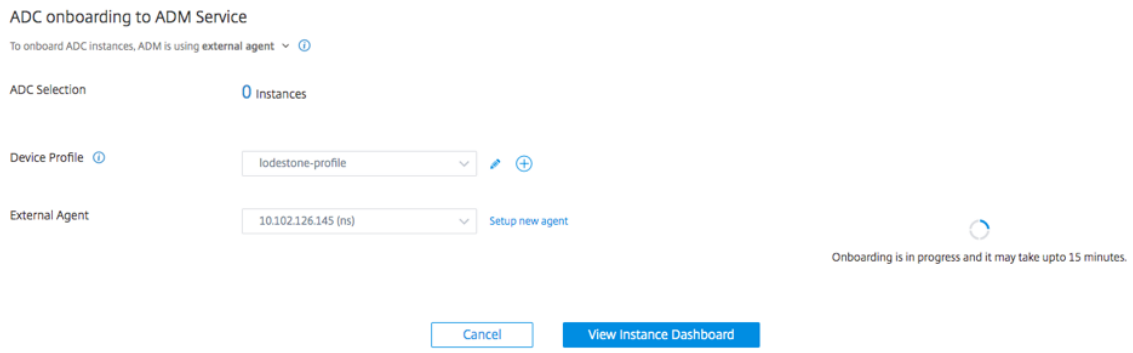


代理使用服务 URL 查找服务，并使用激活代码向服务注册。有关在本地虚拟机管理程序上安装代理的详细说明，请参见本地 安装 NetScaler 代理

4. 单击 注册代理。完成后，单击“完成”返回 NetScaler 入门 NetScaler 控制台页面。



5. 单击“开始登录”。载入所有实例后，单击“查看实例面板”转到 NetScaler 控制台实例管理用户界面控制面板并探索不同的功能。



在公有云上安装代理

您可以在以下云环境之一中安装代理：

- Amazon Web Services
- Microsoft Azure
- Google 云端平台

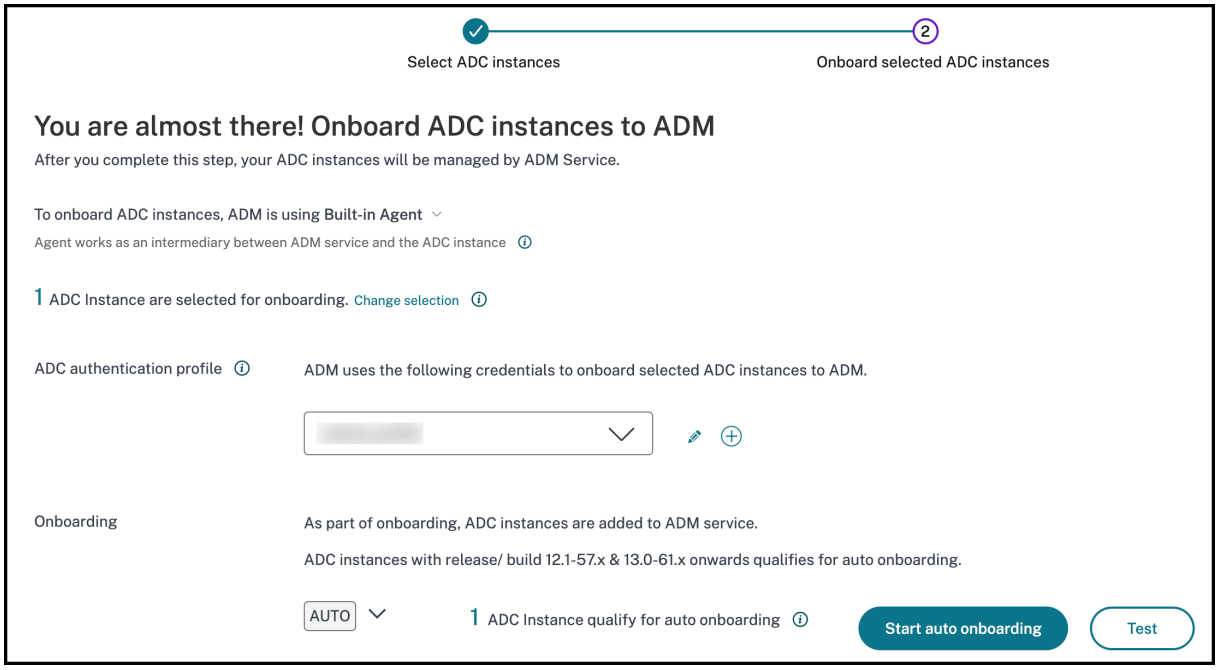
有关详细信息，请参阅以下文档：

- 在 Microsoft Azure 云上安装代理
- 在 AWS 上安装代理
- 在 GCP 上安装代理

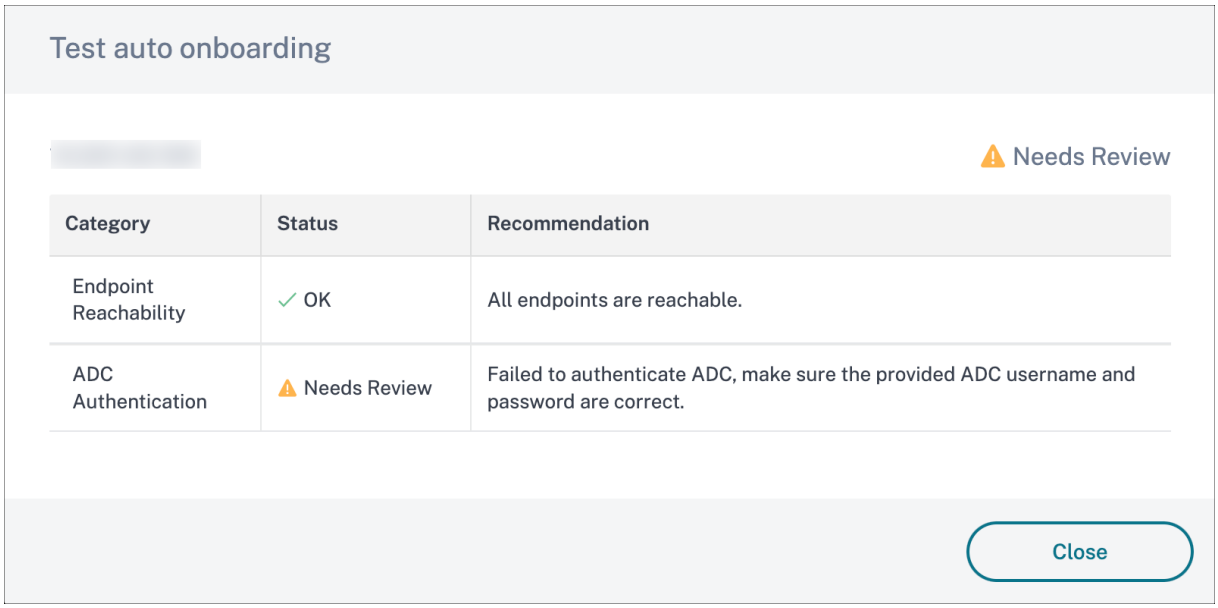
测试 **NetScaler** 实例的入门准备情况

September 2, 2024

当您想要将 NetScaler 实例加载到 NetScaler 控制台时，可以测试这些实例是否已准备就绪，可以开始使用。测试运行状态会提示您实例是否已准备就绪或需要审查。



单击“测试”开始诊断试运行。测试自动入门 页面显示问题类别、状态和建议。



有关更多信息，请参见在 NetScaler 控制台 GUI 中查看 NetScaler 诊断信息。

如果 NetScaler 测试运行状态为“需求审查”状态，那么：

- 查看“设备配置文件”中的 NetScaler 登录凭据。
- 以下端点无法到达：
  - adm.cloud.com
  - agent.adm.cloud.com
  - trust.citrixnetworkapi.net
  - download.citrixnetworkapi.net

如果您在运行登录准备测试时遇到任何问题，请参阅 故障排除 以获取建议。

电子邮件设置

January 29, 2024

NetScaler 控制台服务允许使用基于 Advisory Concole Connect 的低接触入门工作流程来加载 NetScaler 实例。作为该工作流程的一部分，客户会收到来自 NetScaler 控制台服务的产品发起的电子邮件。您可以启用或禁用在基于 Advisory Connect 的低接触入职工作流程中收到的电子邮件通知。您可以通过以下方式配置和管理电子邮件通知：

- 为所有管理员启用电子邮件 -您将能够为组织中的所有管理员启用电子邮件。默认情况下，为组织中的所有管理员启用电子邮件。
- 启用/禁用选定管理员的电子邮件 -您可以自定义电子邮件设置，以便只有组织中的特定管理员接收电子邮件，而其他管理员不接收电子邮件。
- 禁用所有管理员的电子邮件-您将能够禁用和停止组织中所有管理员的电子邮件。

配置电子邮件设置

您可以配置电子邮件设置，启用或禁用在基于 Console Advisory Connect 的低接触入门工作流程中收到的电子邮件。要配置 电子邮件设置，请执行以下操作：

1. 在产品发起 的电子邮件中单击“加入 **ADM** 服务”。将出现 **Citrix Cloud** 页面。
2. 在 **Citrix Cloud** 登录页面中：
   - 如果您是 Citrix Cloud 的现有客户，请使用您的 Citrix.com、My Citrix 或 Citrix Cloud 凭据登录 Citrix Cloud。
   - 如果您不是 Citrix Cloud 的现有客户，请注册 Citrix Cloud。有关更多信息，请参阅 注册 Citrix Cloud。

> 注意：
>
> 如果您是多个组织 ID 的一员，并且其中一个组织 ID 在 Citrix Cloud 中，请使用现有凭据登录。

此时将出现 NetScaler 控制台登录页面，向您概述了 NetScaler 控制台及其优点。

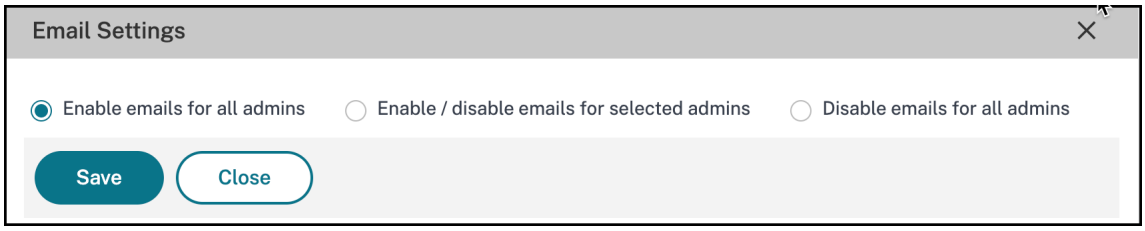
3. 在 NetScaler 控制台登录页面中，单击“下一步”。

   此时将显示“对您的 **NetScaler** 和网关 实例的见解”页面，您可以在其中深入了解整个 NetScaler 基础架构并提供建议。

4. 在 **NetScaler** 和网关实例的见解页面中，单击“下一步”。

   将出现“选择要载入的 **NetScaler** 和网关实例”页面，您可以在其中看到要加载的 NetScaler 实例列表以及其他选项，例如电子邮件设置。

5. 单击“电子邮件设置”。将出现“电子邮件设置”窗格。



   现在，您可以配置电子邮件设置以启用或禁用电子邮件。

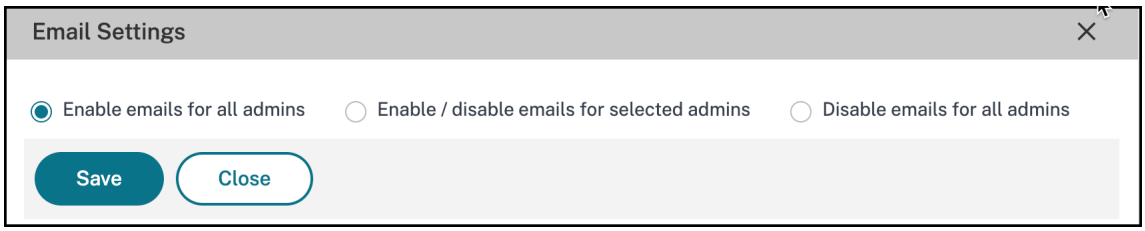
> 注意：
>
> 如果您只加载了一个 NetScaler 实例，则不会收到这些邮件。

如果您已经在使用 NetScaler 控制台 GUI 并且想要配置电子邮件设置：

1. 在 NetScaler 控制台 GUI 中，导航 到 基础架 构 实例，然后单击 **NetScaler**。将出现 **NetScaler** 页面。
2. 在 **NetScaler** 页面中，单击“资产清单”。

   此时将出现“选择要载入的 **NetScaler** 和网关实例”页面，其中显示了已载入的 NetScaler 实例列表以及其他选项，例如电子邮件设置。

3. 单击“电子邮件设置”。将出现“电子邮件设置”窗格。



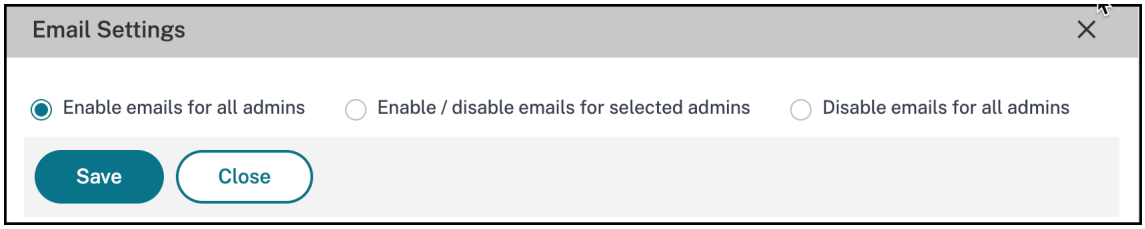
   现在，您可以配置电子邮件设置以启用或禁用电子邮件。

为所有管理员启用电子邮件

默认情况下，为组织中的所有管理员启用电子邮件。

要在基于控制台公告连接的工作流程中启用或订阅电子邮件通知，请执行以下操作：

1. 在“电子邮件设置”窗格中，选择“为所有管理员 启用电子邮件”。



2. 单击保存和关闭。

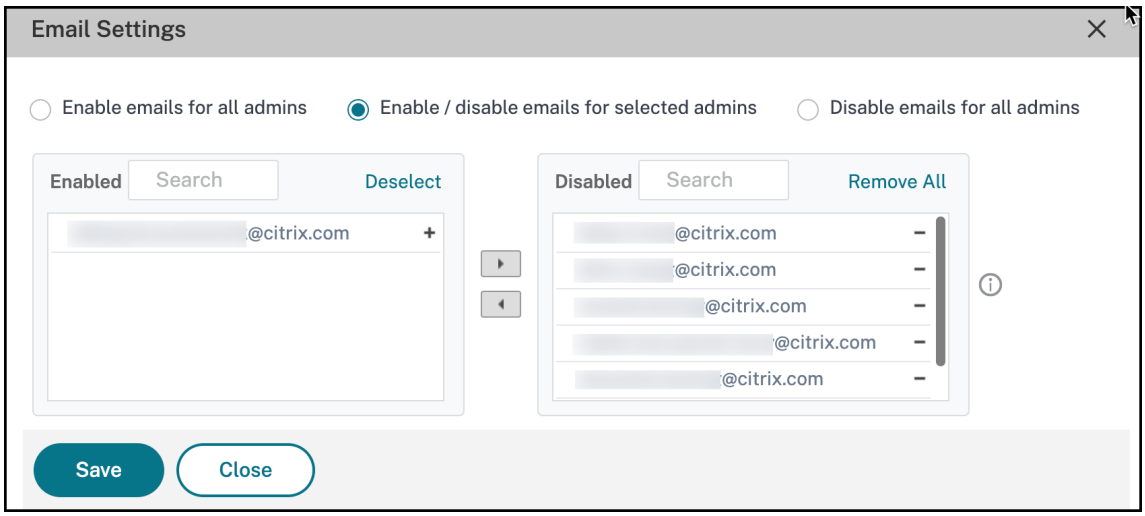
   组织中的所有管理员现已订阅，并将作为基于控制台公告连接的工作流程的一部分收到电子邮件通知。

启用/禁用组织中特定管理员的电子邮件

您可以自定义电子邮件设置，以便只有组织中的特定管理员才能收到电子邮件。您将在左侧看到启用电子邮件的管理员列表，在右侧看到禁用电子邮件的管理员列表。

要禁用组织中特定管理员的电子邮件，请执行以下操作：

1. 在“启用”列表中找到管理员电子邮件地址。
2. 单击“添加”按钮 (**+**)。



   您将看到管理员电子邮件地址已添加到“禁用”列表中。

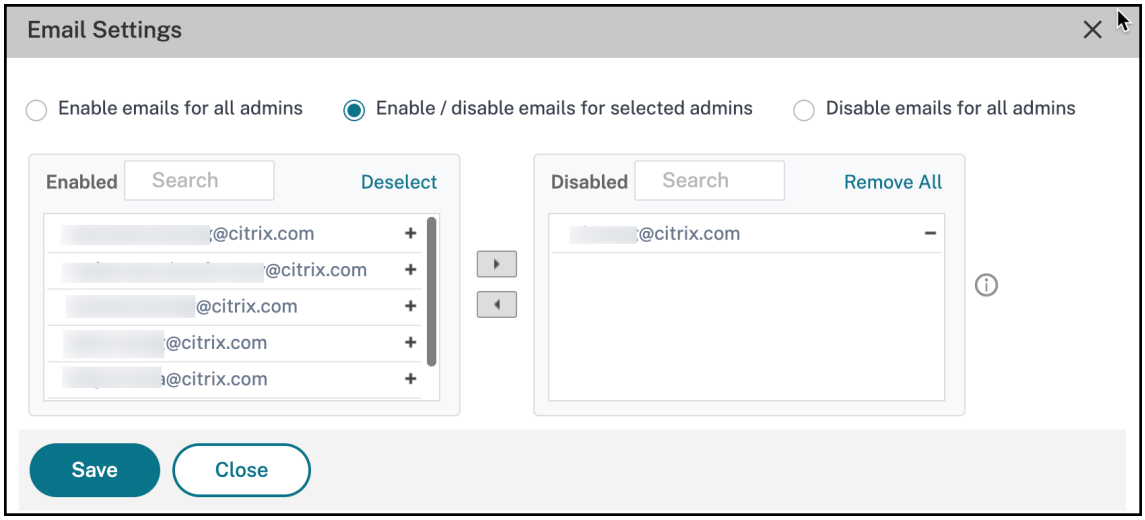
3. 单击保存和关闭。

   作为基于控制台公告连接的工作流程的一部分，管理员现已取消订阅，无法接收电子邮件通知。

> 注意：
>
> 如果您想为多个管理员禁用电子邮件，请在“启用的 电子邮件”列表中选择他们的所有电子邮件 ID，然后单击“添加”按钮 (+) 将电子邮件 ID 添加到“已禁用”列表中 **。单击保存和关闭 **。

如果您之前禁用了组织中特定或所有管理员的电子邮件，则可以为所有管理员启用电子邮件。要为组织中的特定管理员启用电子邮件，请执行以下操作：

1. 在“禁用”列表中找到管理员电子邮件地址。
2. 单击“移除”按钮 (-)。您将看到管理员电子邮件地址已从“禁用”列表中删除。



3. 单击保存和关闭。

   管理员现在将开始接收与登录相关的电子邮件。管理员现已订阅接收电子邮件通知。

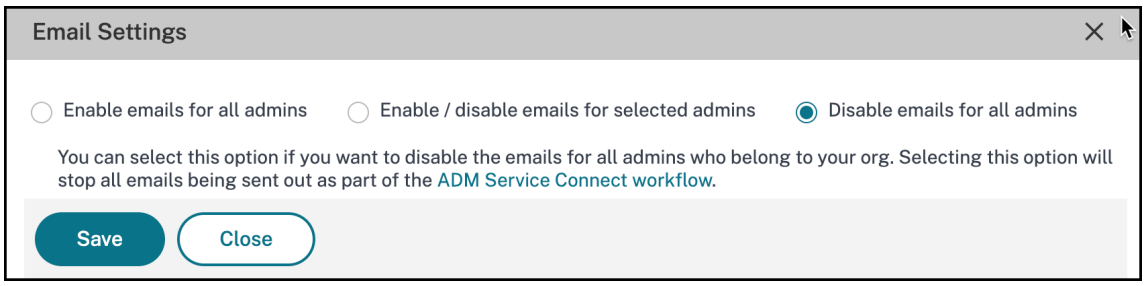
> 注意：
>
> 如果您想为多个管理员启用电子邮件，请在“已禁用的 电子邮件”列表中选择他们的所有电子邮件 ID，然后单击“移除”按钮 (-) 将电子邮件 ID 添加到“启用”列表中 **。单击保存和关闭 **。

禁用所有管理员的电子邮件

如果您想禁用或停止向属于您的组织的所有管理员发送电子邮件，则可以选择此选项。

要禁用或取消订阅接收电子邮件，请执行以下操作：

1. 在“电子邮件设置”窗格中，选择“为所有管理员禁用电子邮件”。



2. 单击保存和关闭。

   组织中的所有管理员现已取消订阅，不会收到任何电子邮件通知。

使用诊断工具或 **NetScaler** 控制台 **GUI** 对问题进行故障排除

January 29, 2024

> 注意
>
> 该诊断工具仅适用于已载入或使用基于控制台公告连接的低接触入门的 NetScaler 实例。
>
> 有关更多信息，请参阅使用 NetScaler 控制台连接以 低接触方式加载 NetScaler 实例。

当您将 NetScaler 实例载入 NetScaler 控制台时，您可能会遇到一些阻碍 NetScaler 实例成功启动的问题。作为管理员，您必须知道登录失败的原因。在以下情况下，您可以使用诊断工具执行诊断检查：

- 在自动登录或基于脚本的登录过程中遇到任何问题
- 想要确保 NetScaler 实例是否已准备就绪
- 想要分析在 NetScaler 控制台 GUI 中显示“关闭”状态的已载入的 NetScaler 实例的问题

如果在 NetScaler 实例上启用了 Console Ad visory Connect，则诊断详细信息将自动发送到 Citrix，您可以在 NetScaler 控制台 GUI 中查看详细信息。如果未启用控制台公告连接，则可以 手动使用诊断工具。

手动使用诊断工具

诊断工具作为 `mastools` 升级（13.1-2.x 或更高版本）的一部分提供，可通过以下 URL 访问：`/var/mastools/scripts`。您可以通过在 `mastools`NetScaler 实例中`cat /var/mastools/version.txt`运行命令来验证 版本。

要运行诊断工具，请执行以下操作：

1. 使用 SSH 客户端登录到 NetScaler 实例。
2. 键入 shell 并按 Enter 键切换到 bash 模式。

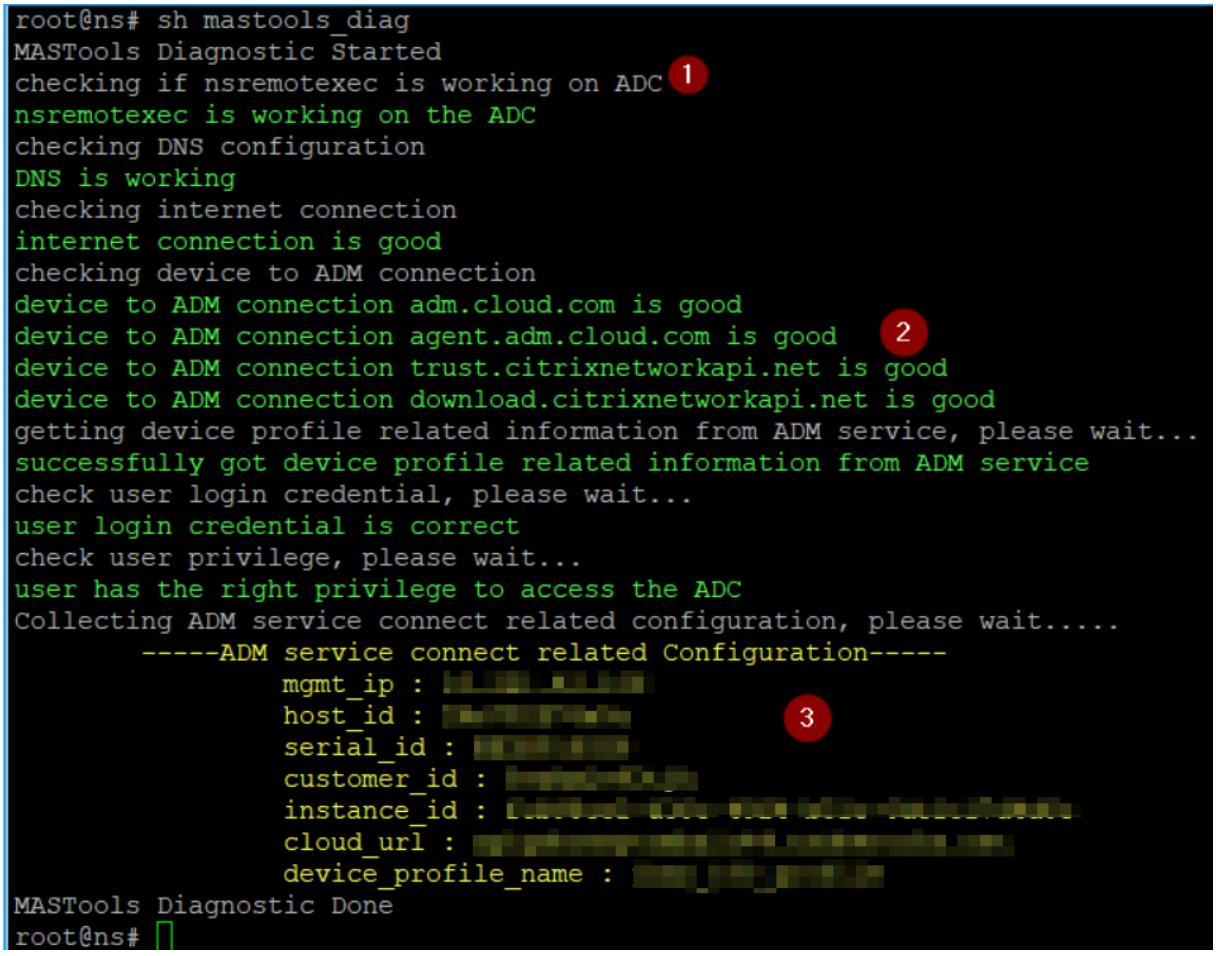
3. 键入 `cd /var/mastools/scripts`。
4. 键入 `sh mastools_diag`。

该工具启动并显示以下诊断检查的结果：

- **nscli**
- **DNS** 配置
- 互联网连接
- 实例到 **ADM** 的连接
- 用户特权

如果故障排除后问题仍然存在，则可以联系支持人员。联系支持部门时，必须提供运行诊断工具后显示的配置信息。

以下是没有问题的 NetScaler 实例的诊断结果示例：

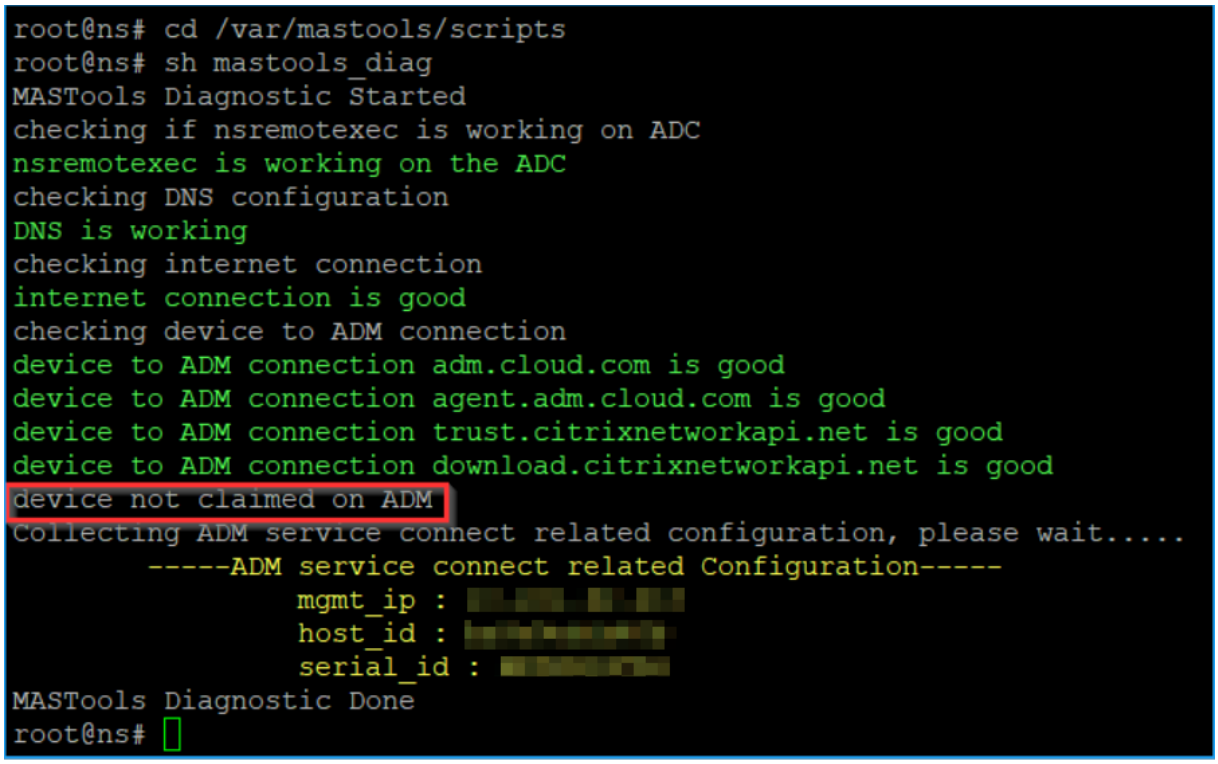


- **1** —显示诊断检查的类型
- **2** —以绿色或红色显示诊断检查结果。绿色表示结果成功，红色表示结果不成功。

- **3**—每次运行诊断工具时，以黄色显示 NetScaler 控制台配置信息。如果您想联系 NetScaler 支持人员，则必须提供此信息。

使用诊断工具验证 **NetScaler** 实例是否已准备就绪，可以上手

在将 NetScaler 实例加载到 NetScaler 控制台之前，您可以通过在 NetScaler 实例上运行诊断工具来检查 NetScaler 实例的准备情况。如果 NetScaler 实例没有问题且已准备就绪，则该工具会显示 **ADM** 上 未申领的设备消息。



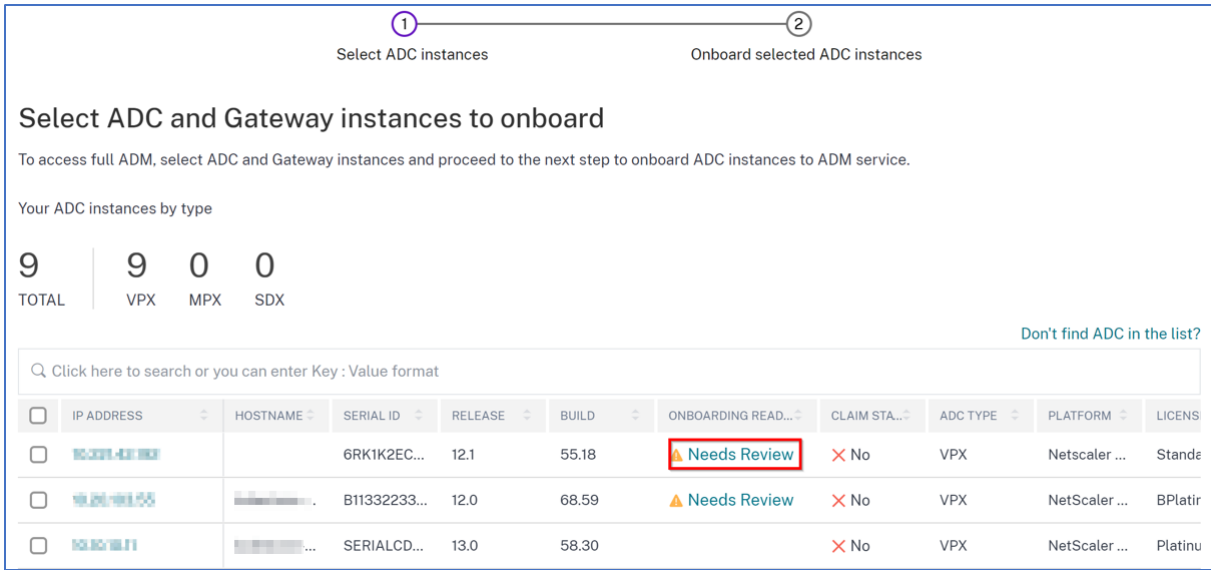
在 **NetScaler** 控制台 **GUI** 中查看 **NetScaler** 诊断信息

导航到基础架构 **>** 实例 **> NetScaler**，然后单击资产清单，查看新添加的入门就绪选项，该选项提供 NetScaler 实例的入门准备状态，例如需求审查或确定。

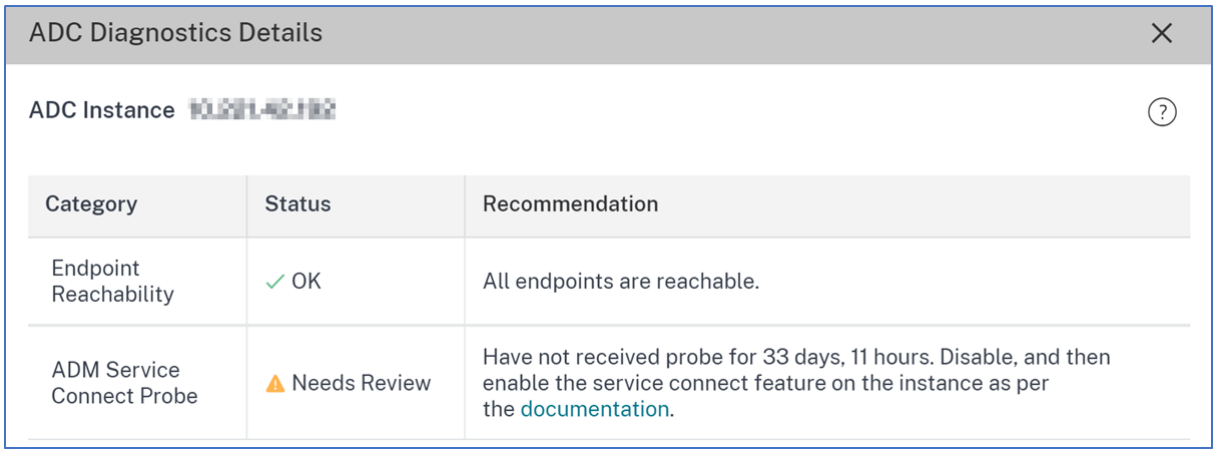
- 需要审查。NetScaler 实例存在需要修复的问题。
- 好吧。NetScaler 实例已准备就绪，可以上手了。

> 注意：
>
> 如果“入门就绪”显示为空白，则表示 NetScaler 实例未使用支持诊断的最新映像运行。

如果 NetScaler 实例有任何问题，将出现“需求 审查”选项，您可以单击查看更多细节。



单击“需要查看”后，**NetScaler** 诊断 详情页面将显示问题详情。



- **Category**（类别）。提供问题类别。
- 状态。提供问题状态，例如“需要审查”、“确定”或“不适用”。
- 建议。提供解决问题所需的建议。

修复问题后，“登录准备就绪”中的状态更改为“正常”。

故障排除

以下是一些 NetScaler 实例问题及其故障排除步骤：

用户名或密码无效

```
root@ns# cd /var/mastools/scripts
root@ns# sh mastools_diag
MASTools Diagnostic Started
checking if nsremotexec is working on ADC
nsremotexec is working on the ADC
checking DNS configuration
DNS is working
checking internet connection
internet connection is good
checking device to ADM connection
device to ADM connection adm.cloud.com is good
device to ADM connection agent.adm.cloud.com is good
device to ADM connection trust.citrixnetworkapi.net is good
device to ADM connection download.citrixnetworkapi.net is good
getting device profile related information from ADM service, please wait...
successfully got device profile related information from ADM service
check user login credential, please wait...
incorrect login credential
Collecting ADM service connect related configuration, please wait.....
        -----ADM service connect related Configuration-----
                mgmt_ip :
                host_id :
                serial_id :
                customer_id :
                instance_id :
                cloud_url :
                device_profile_name :
946_profile
MASTools Diagnostic Done
root@ns#
```

解决方法：确保管理员配置文件中提供的用户名和密码正确无误。如果您修改了 NetScaler 实例密码，则必须修改实例的管理配置文件。有关更多信息，请参阅 修改管理员配置文件。

DNS 配置错误

```
root@ns# sh mastools_diag
MASTools Diagnostic Started
checking if nsremotexec is working on ADC
nsremotexec is working on the ADC
checking DNS configuration
Problem in DNS setting, could not resolve test host.
Have you configured name server on your ADC? Please make sure DNS is configured
and working
Collecting ADM service connect related configuration, please wait.....
        -----ADM service connect related Configuration-----
                mgmt_ip :
                host_id :
                serial_id :
MASTools Diagnostic Done
root@ns#
```

解决方法：确保 DNS 已配置或者 DNS IP 地址有效。有关更多信息，请参阅 DNS 配置。

没有互联网连接

解决方法：确保防火墙设置没有阻止 Internet 访问，并且配置了所需的代理。

无法连接到 **NetScaler** 控制台端点

解决办法：确保检查防火墙设置，并且防火墙中未阻止以下 NetScaler 控制台端点：

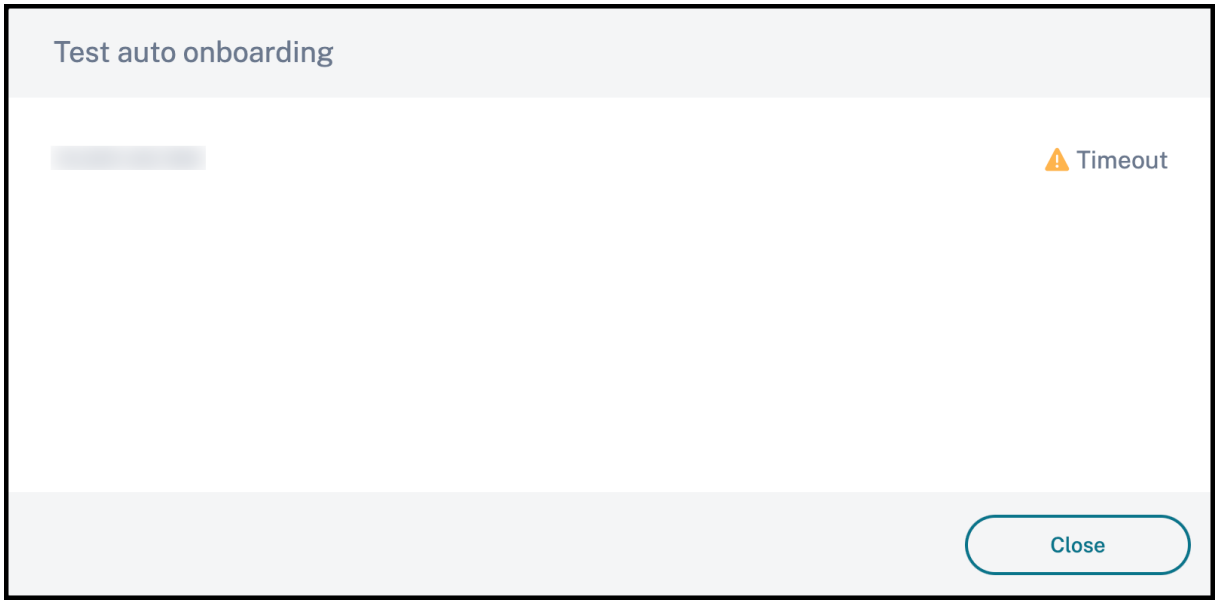
```
ADM_GRP_EP = "adm.cloud.com"

ADM_AGENT_EP = "agent.adm.cloud.com"

ADM_TRUST_EP = "trust.citrixnetworkapi.net"

ADM_DOWNLOAD_EP = "download.citrixnetworkapi.net"
```

如果在诊断检查中未发现问题且无连接问题仍然存在，请记下 NetScaler 控制台配置信息（以黄色显示）并联系 NetScaler 支持部门。

当您执行测试运行以确保 NetScaler 实例准备就绪时，可能会出现以下问题：

内置代理试运行超时

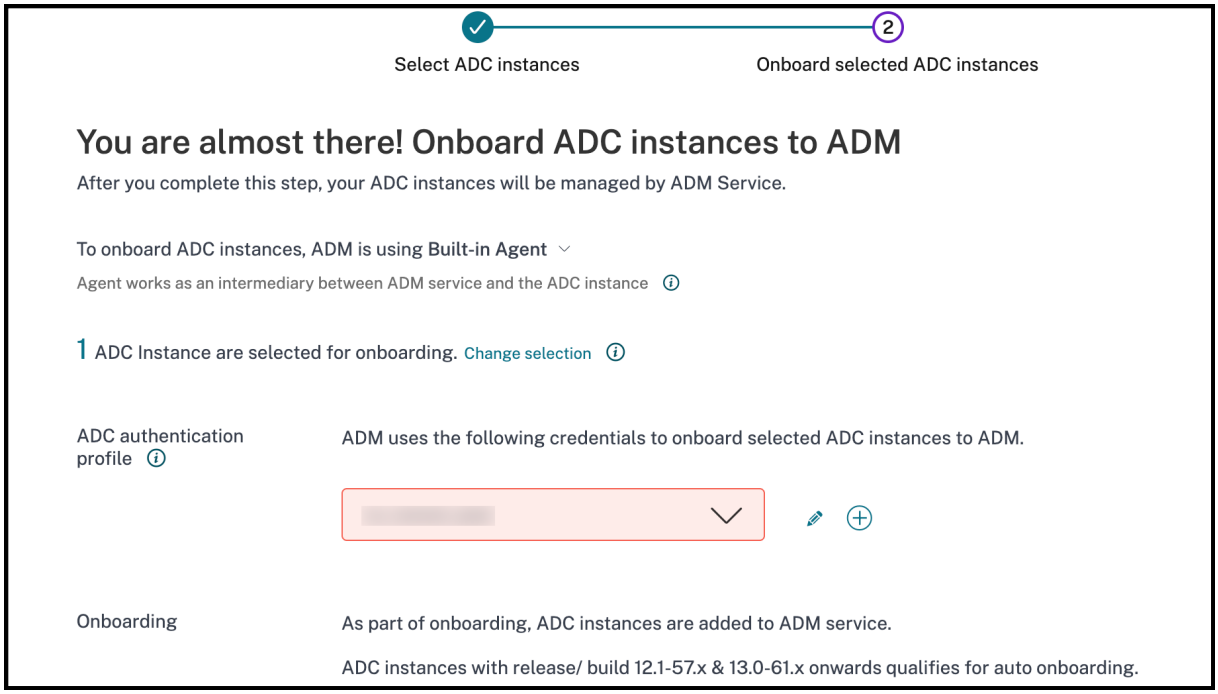
如果在 5 分钟内未提取试运行结果，则会显示超时消息。



建议：建议您验证 NetScaler 实例是否使用支持诊断的最新映像运行。此外，在资产选择表中，登录准备情况列显示为空白。

设备配置文件下拉列表中的红色轮廓

NetScaler 认证在试运行期间失败，设备配置文件下拉列表中会显示红色轮廓。



建议：再次重新输入 NetScaler 用户管理凭据，创建设备配置文件并单击“测试”再次运行试运行。

从内置代理过渡到外部代理

January 29, 2024

您可能一开始仅使用 NetScaler 控制台进行管理和监视，之后可能需要使用其他功能，例如池化许可和分析。为此，必须从内置代理过渡到外部代理。

内置代理仅支持管理和监视功能。对于其他 NetScaler 控制台功能，例如池化许可和分析，您需要外部代理。本文档介绍了从现有 NetScaler 控制台内置代理过渡到基于外部虚拟机管理程序的代理的步骤。

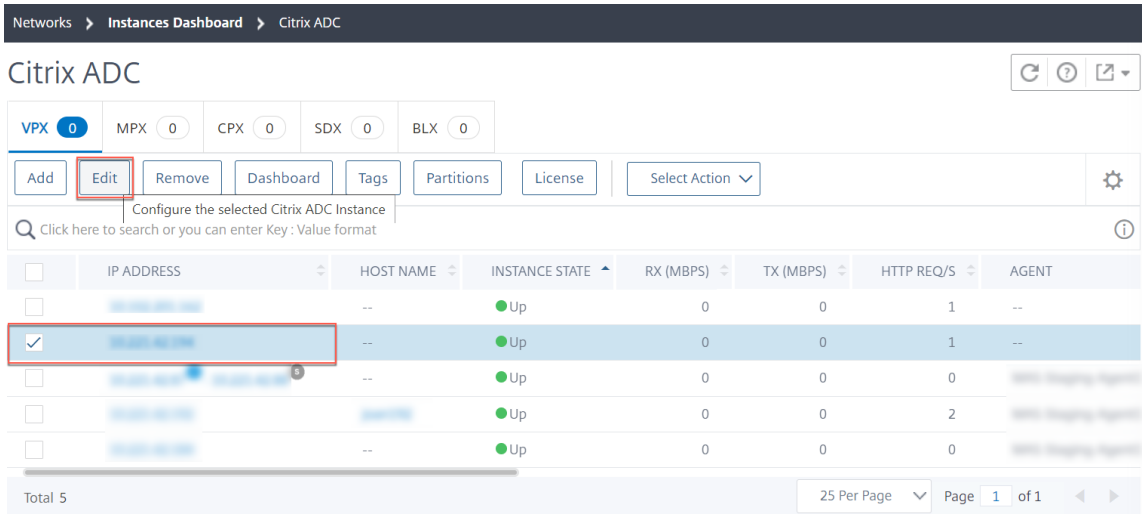
开始之前的准备工作

在开始转换之前安装外部代理。按照在本地 安装 NetScaler 代理主题中提供的步骤进行操作。

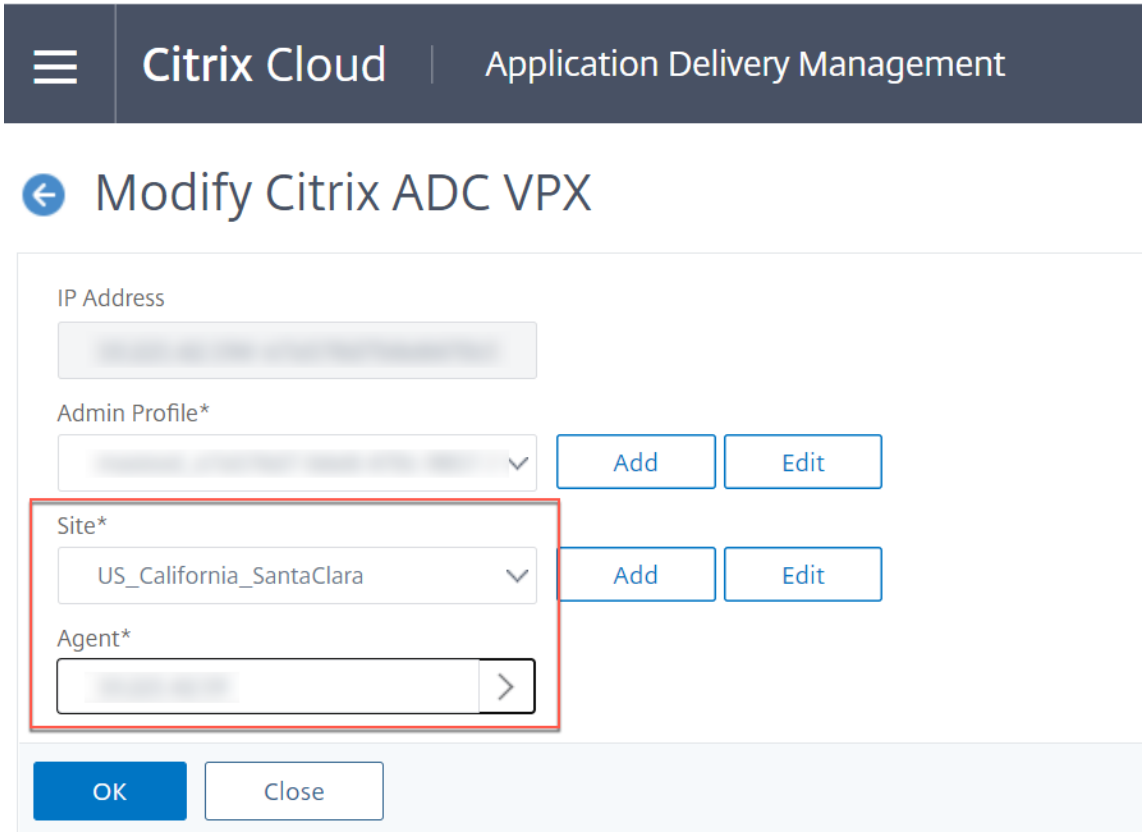
从内置代理过渡到外部代理

请按照以下步骤从内置代理过渡到外部代理：

1. 在 NetScaler 控制台 GUI 中，在 基础架构 **>** 实例控制面板 **> NetScaler** 下，选择 NetScaler 实例，然后单击 “*** 编辑”。



2. 选择站点和代理，然后单击“确定”。



3. 再次选择实例，然后单击 选择操作 **>** 重新发现。

有关如何在 NetScaler 控制台中创建站点并将代理添加到站点的信息，请参见添加实例

将 **SAML** 作为身份提供者连接到 **NetScaler** 控制台

January 29, 2024

NetScaler 控制台支持使用 SAML（安全断言标记语言）作为身份提供者对登录其 NetScaler 控制台的管理员和订阅者进行身份验证。您可以将自己选择的 SAML 2.0 提供程序与本地 Active Directory (AD) 配合使用。

对于大多数 SAML 提供商，请使用本文中的信息设置 SAML 身份验证。如果您想在 Azure AD 中使用 SAML 身份验证，您可以选择使用 Azure AD 应用程序库中的 Citrix Cloud SAML SSO 应用程序。

必备条件

使用 NetScaler 控制台进行 SAML 身份验证具有以下要求：

- 支持 SAML 2.0 的 SAML 提供商
- 本地 AD 域
- 两个 Cloud Connector 部署到资源位置并加入到您的本地 AD 域。Cloud Connector 用于确保 Citrix Cloud 可以与您的资源位置进行通信。
- 与您的 SAML 提供商的 AD 集成。

Cloud Connector

您必须至少有两 (2) 台服务器才能安装 Citrix Cloud Connector 软件。建议至少有两台服务器以实现 Cloud Connector 的高可用性。这些服务器必须满足以下要求：

- 符合 Cloud Connector 技术详情中描述的系统要求。
- 未安装任何其他 Citrix 组件，不是 AD 域控制器，也不是对资源位置基础架构至关重要的计算机。
- 已加入您的资源所在的域。如果用户访问多个域中的资源，则必须在每个域中至少安装两个 Cloud Connector。
- 已连接到可以联系订阅者通过 Citrix Workspace 访问的资源的网络。
- 已连接到 Internet。

Active Directory

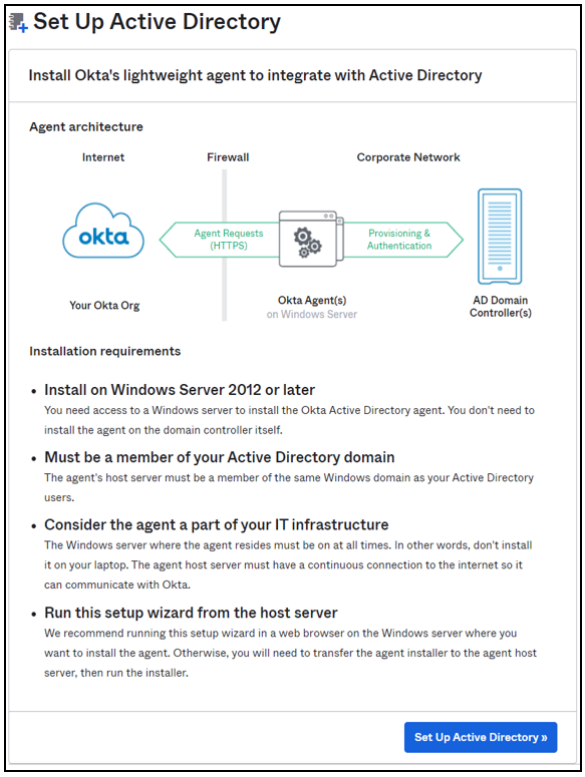
在配置 SAML 身份验证之前，请执行以下任务：

- 要将用户导入 Okta 实例，Active Directory 中的用户必须填写名字、姓氏和电子邮件字段。
- 验证您的工作区订阅者在 Active Directory (AD) 中是否有用户帐户。配置 SAML 身份验证后，没有 AD 帐户的订阅者无法成功登录其工作区。

- 确保已填充订阅者 AD 帐户中的用户属性。订阅者登录 Citrix Workspace 时，Citrix Cloud 需要这些属性来建立用户上下文。如果未填充这些属性，则订阅者将无法登录。这些属性包括：
  - 电子邮件地址
  - 显示名称（可选）
  - 常见的名字
  - SAM 帐户名
  - 用户主体名称
  - 对象 GUID
  - SID
- 通过在本地 AD 中部署 Cloud Connector，将 Active Directory (AD) 连接到 Citrix Cloud 帐户。
- 将您的 AD 用户与 SAML 提供商同步。Citrix Cloud 要求您的 Workspace 订阅者具有 AD 用户属性，以便他们能够成功登录。

SAML 单点登录

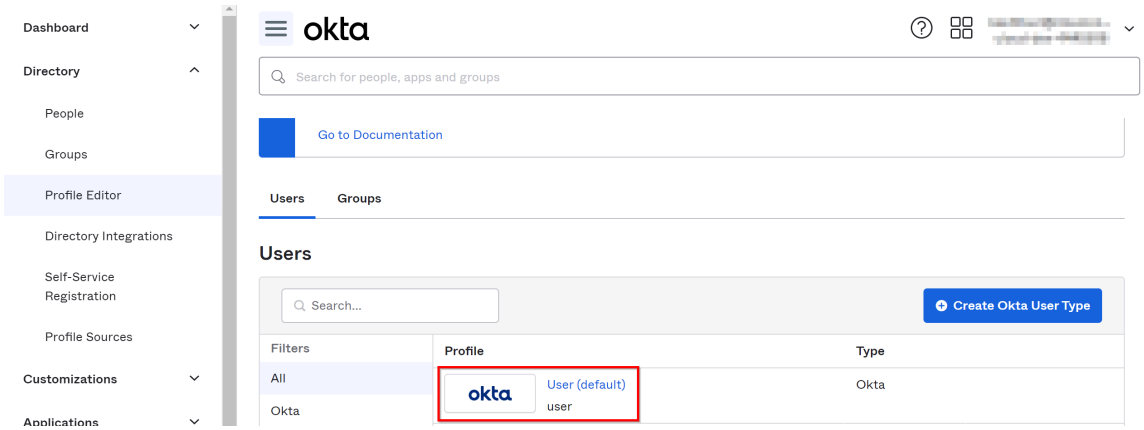
在 Okta 实例中，导航到目录集成 **>** 添加 **Active Directory**。



为了成功集成，SAML 身份提供商必须在 SAML 断言中传递 Citrix Cloud 用户的某些 Active Directory 属性。具体而言，

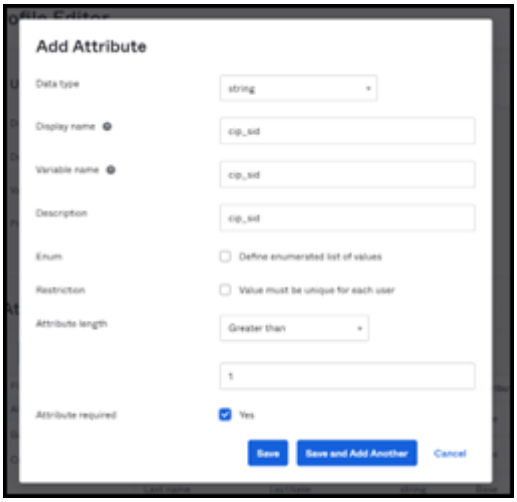
- 安全标识符 (SID)
- objectGUID (OID)
- 用户主体名称 (UPN)
- 邮件（电子邮件）

1. 使用管理员凭据登录到 Okta。
2. 选择“目录”**>**“配置文件编辑器”，然后选择 **Okta** 用户（默认）配置文件。Okta 显示用户配置文件页面。



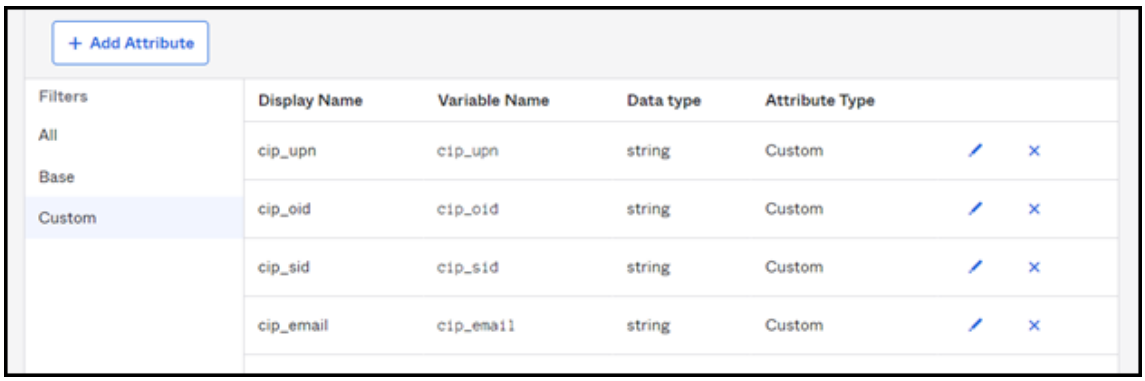
3. 在“属性”下，选择“添加属性”，然后添加自定义字段。

   - `cip_sid`
   - `cip_upn`
   - `cip_oid`
   - `cip_email`



   单击“保存并添加另一个”，然后重复该过程创建 4 个自定义属性。

   创建 4 个自定义属性后，您可以查看以下详细信息：

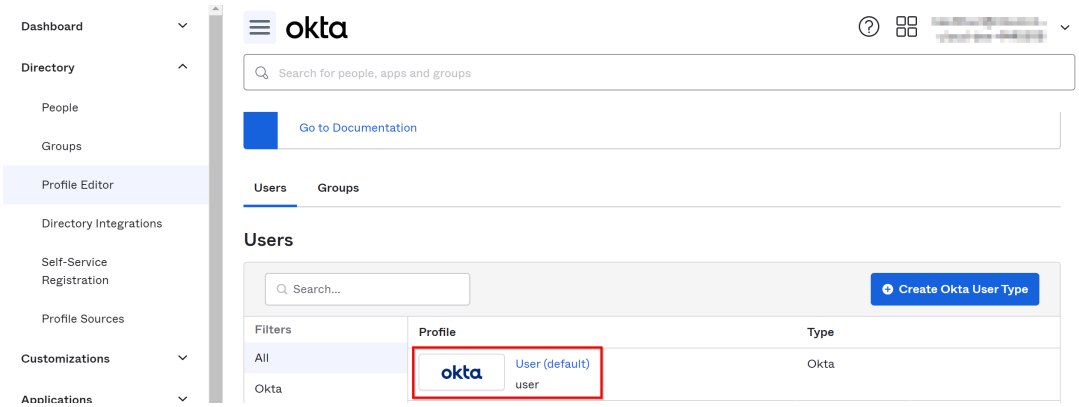


4. 将 Active Directory 属性映射到自定义属性。在用户 **>** 目录下选择您正在使用的 Active Directory。
5. 编辑属性映射：

   a) 在 Okta 控制台中，导航到“目录”**>**“配置文件编辑器”。

   b) 找到您的 AD 的 `active_directory` 配置文件。此配置文件可能使用 myDomain User 格式进行标记，其中 myDomain 是您的集成 AD 域的名称。

   c) 选择“映射”。将显示您的 AD 域的“用户个人资料映射”页面，并选中用于将 AD 映射到 Okta 用户的选项卡。



   d) 在 **Okta** 用户个人资料列中，将 Active Directory 属性映射到您创建的自定义属性：

      i. 对于 `cip_email`，请从域的“用户个人资料”列中选择电子邮件。选中后，映射将显示为 `appuser.email`。

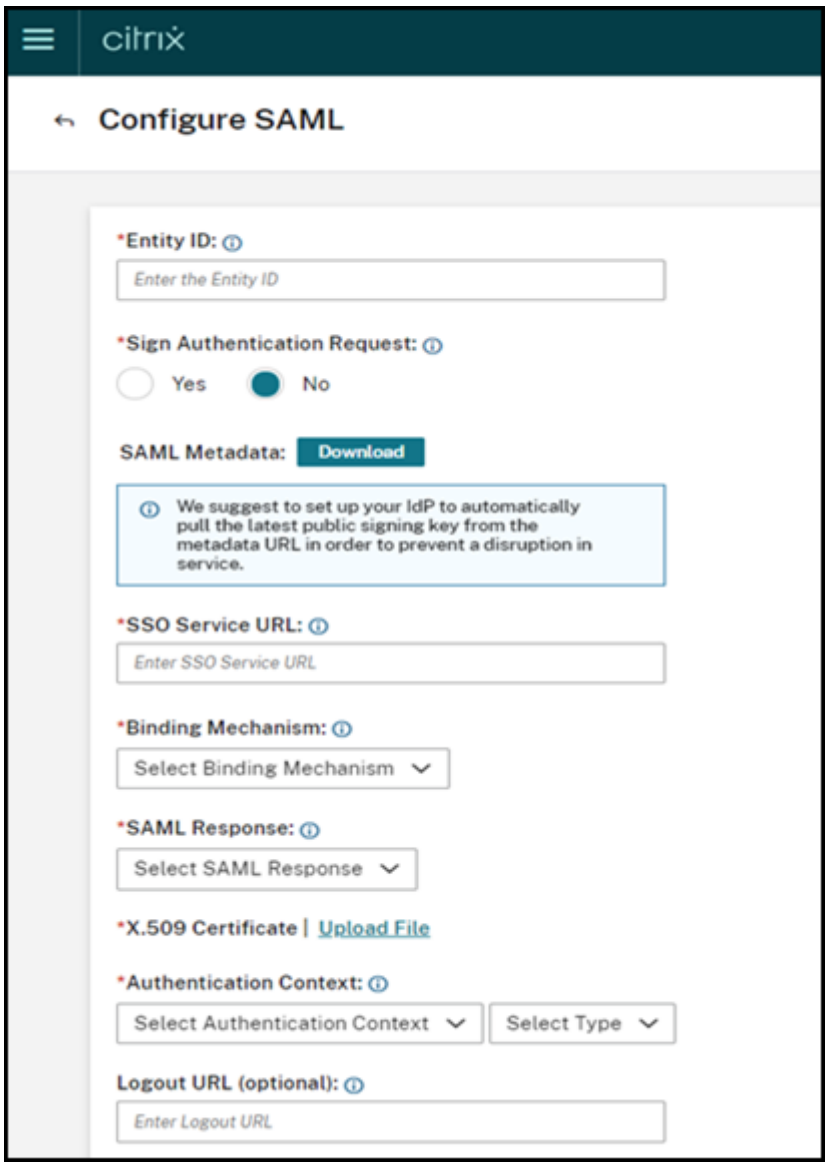
      ii. 对于 `cip_sid`，请从您的域的“用户个人资料文件”列中选择 **ObjectSid**。选中后，映射将显示为 `appuser.objectSid`。

      iii. 对于 `cip_upn`，从域名的“用户资料”列中选`userName`择。选中后，映射将显示为 `appuser.userName`。

      iv. 对于 `cip_oid`，从域名的“用户资料”列中选`externalId`择。选中后，映射将显示为 `appuser.externalId`。

6. 登录到 Citrix Cloud，网址为 `https://citrix.cloud.com`。
7. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
8. 找到 **SAML 2.0** ，然后单击“连接”。

   屏幕上将显示“配置 **SAML**”页面。



   下载 `xml` 文件并使用任何文件编辑器打开文件。在 Okta 中完成进一步配置后，必须再次返回此页面。

9. 在 Okta 中，导航到“应用程序”**>**“创建应用程序集成”。
10. 在“添加应用程序”页面中，单击“创建新应用程序”。
11. 在“创建新的应用程序集成”页面中，选择 **SAML 2.0** ，然后单击“创建”。
12. 提供应用程序名称、应用程序徽标（可选）等详细信息，设置应用程序的可见性，然后单击“下一步”。
13. 在“配置 **SAML**”选项卡中，必须使用下载的 `xml` 文件中的详细信息：

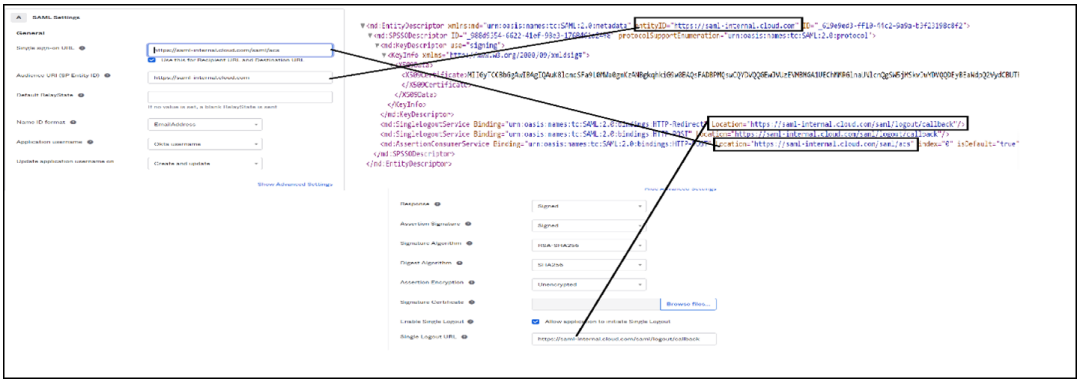
    a) 将单点登录 **URL** 的 URL 详细信息作为 `https://saml-internal.cloud.com/saml/acs` 提供，将受众 **URI**（**SP** 实体 **ID**）的 URL 详细信息作为 `https://saml-internal.cloud.com` 提供。

    > 注意：
    >
    > 如果是外部 Citrix Cloud，则 URL 必须是 `https://saml.cloud.com/saml/acs` 和 `https://saml.cloud.com`，而非 `https://saml-internal.cloud.com` 域。

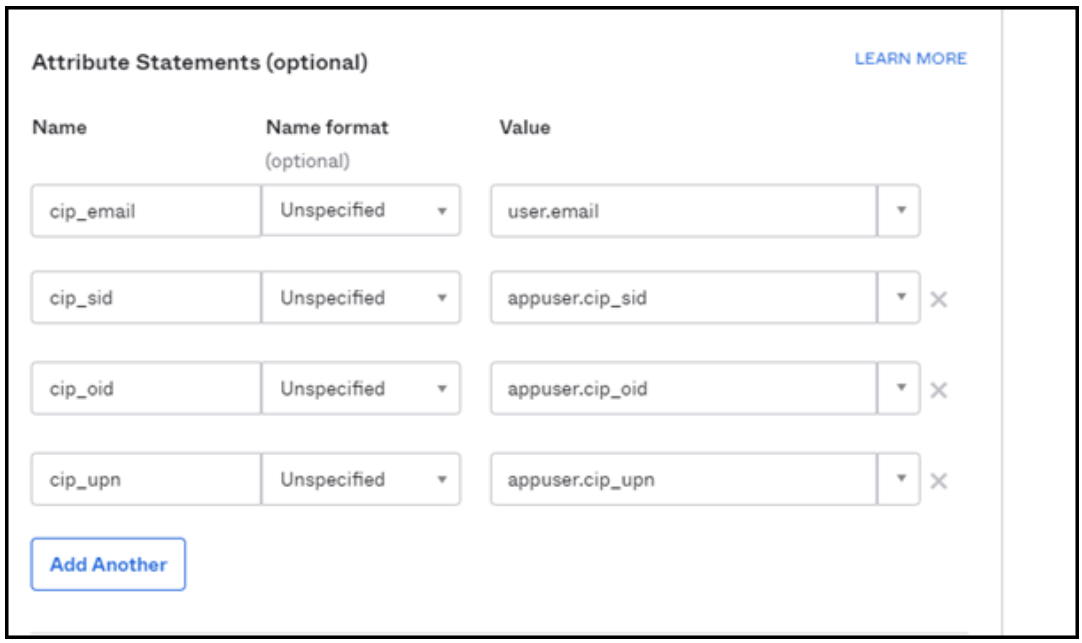
    b) 为“名称 **ID** 格式”选择“未指定”。

    c) 选择 **Okta** 用户名 作为 应用程序用户名。

    d) 单击“显示高级设置”，并确保选择“响应和断言”和“已签名”。



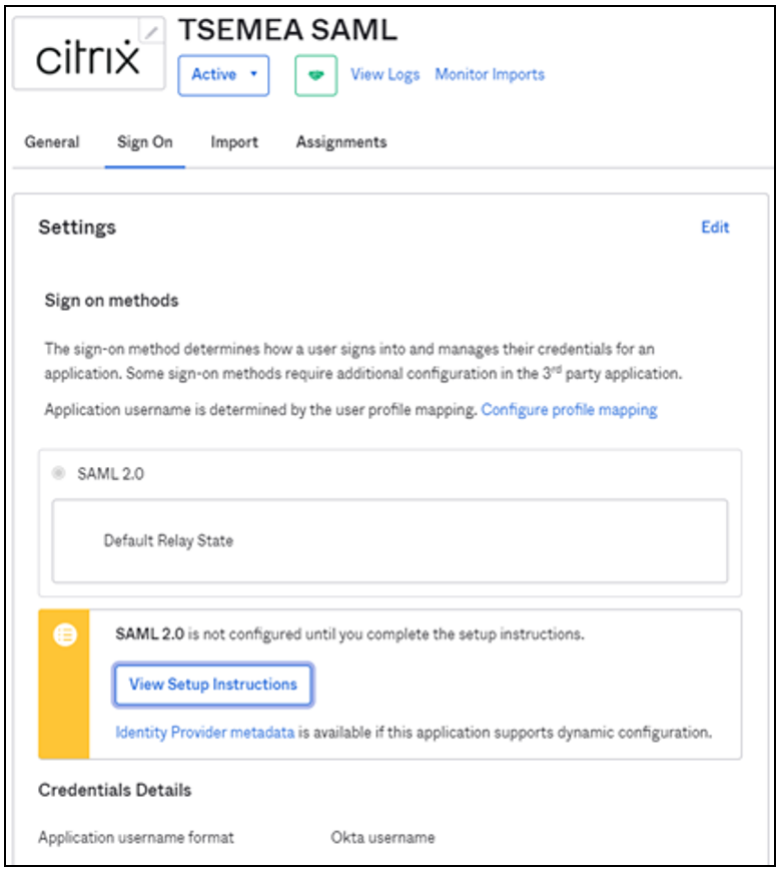
    e) 添加属性语句，如下图所示。



f) 默认情况下，您可以保留所有其他选项，然后单击“下一步”。

g) 选择“我是 **Okta** 客户”，添加内部应用程序，然后单击“完成”。

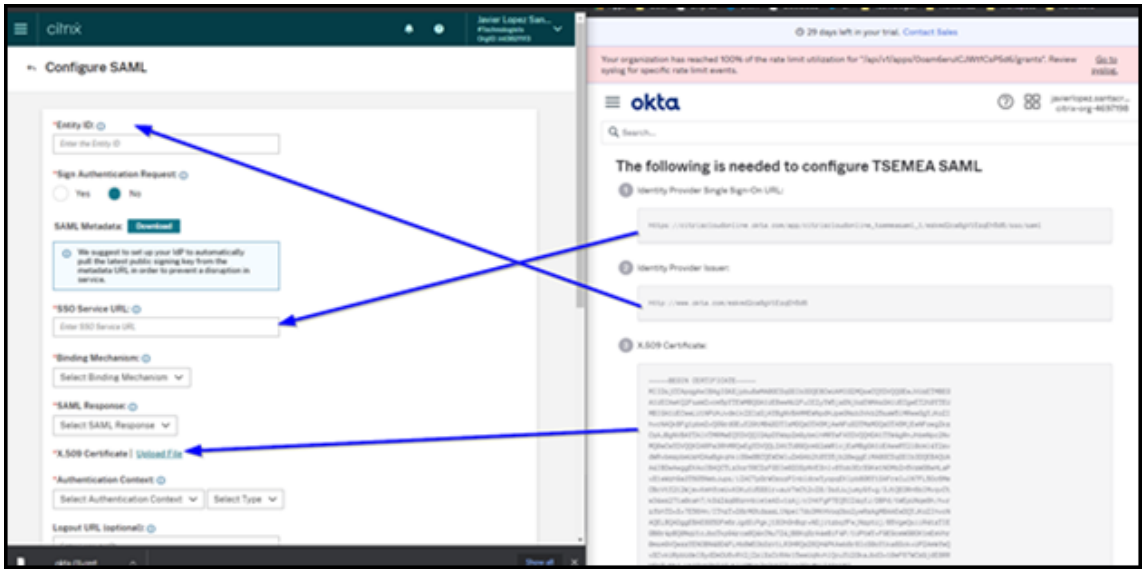
14. Okta 应用程序现已创建，然后单击“查看安装说明”。



将显示“如何为测试应用程序配置 **SAML 2.0**”页面，其中包含您必须再次将其添加到 Citrix Cloud 中的详细信息。

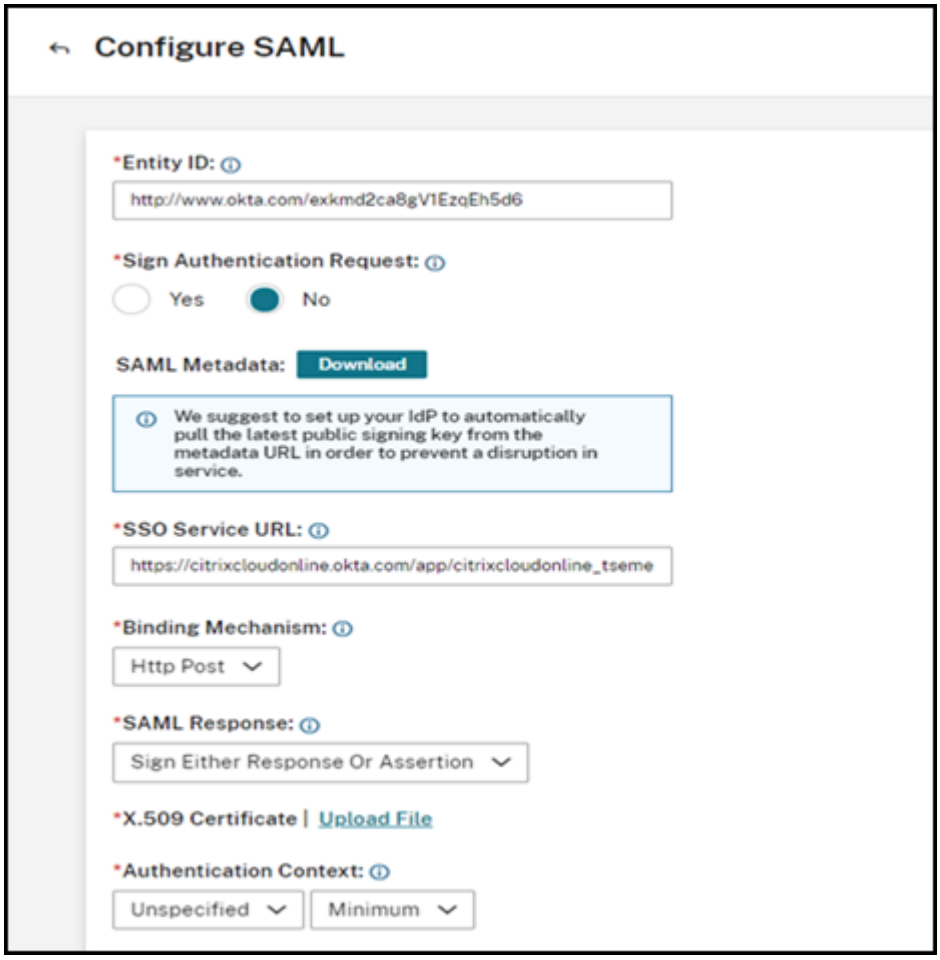
下载证书将其上载到 Citrix Cloud 中。

15. 现在，您必须返回 Citrix Cloud 中的“配置 **SAML**”页面，完成剩余配置，如下所述：

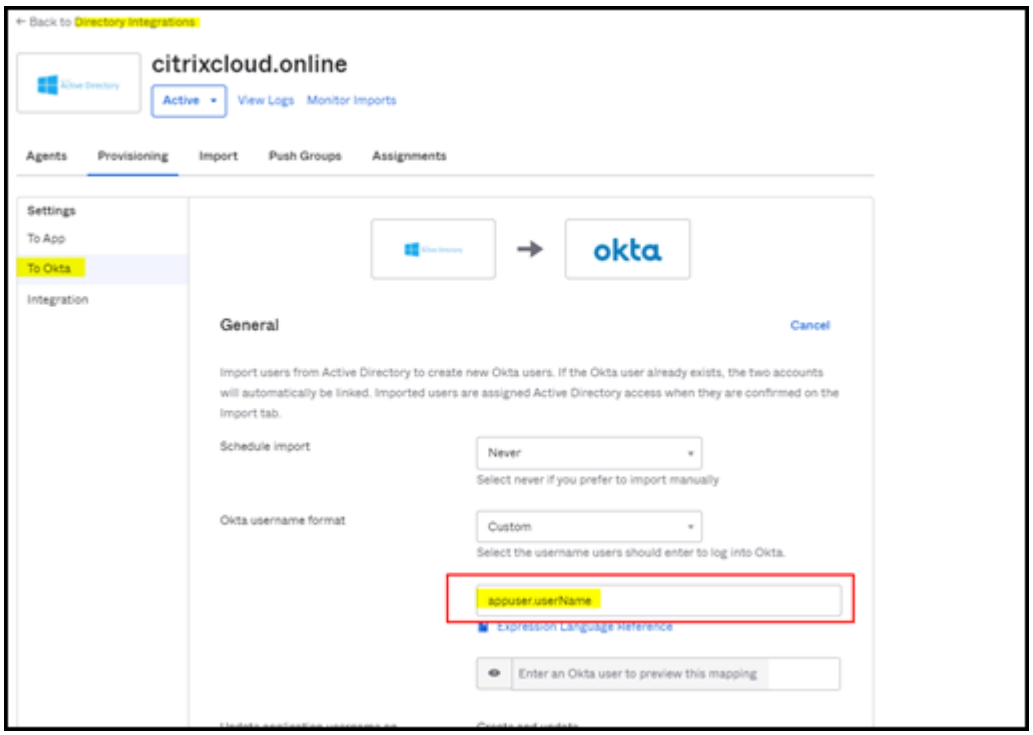


使用下载的证书并将文件扩展名从 `.cert` 重命名为 `.crt`，将其上载到 Citrix Cloud。

16. 上载证书后，使用所有其他默认选项：



17. 接下来，您必须确保 `appuser.userName` 是在目录集成 **> Active Directory ->** 预配 **>** 至 **okta** 上定义的。



> 注意：
>
> 有时，您必须使用 `user.cip_upn` 来代替 `appuser.cip_upn`。确保在 OKTA 集成中验证应用程序的定义，如下图所示。

18. 现在，您必须尝试将 Okta 中的用户添加到此 SAML 应用程序。您可以通过多种方式分配用户。

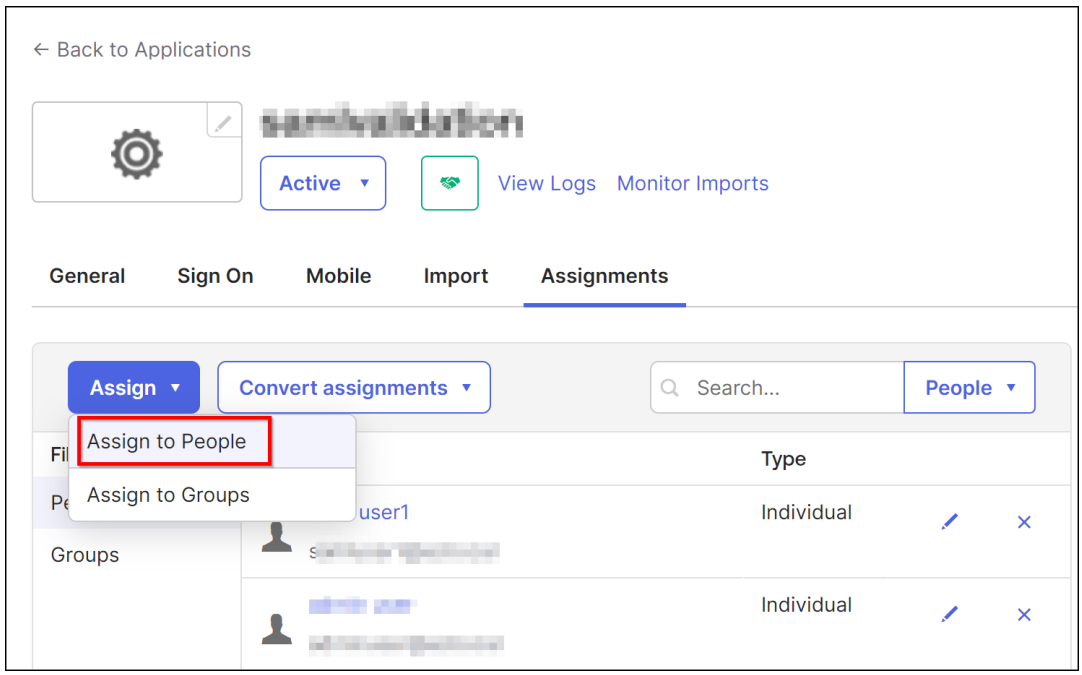
    方法 **1**：

    a) 使用管理员凭据登录 Okta

    b) 导航到“应用程序”**>**“应用程序”

    c) 选择您创建的 SAML 应用程序

    d) 单击“分配”**>**“分配给人员”



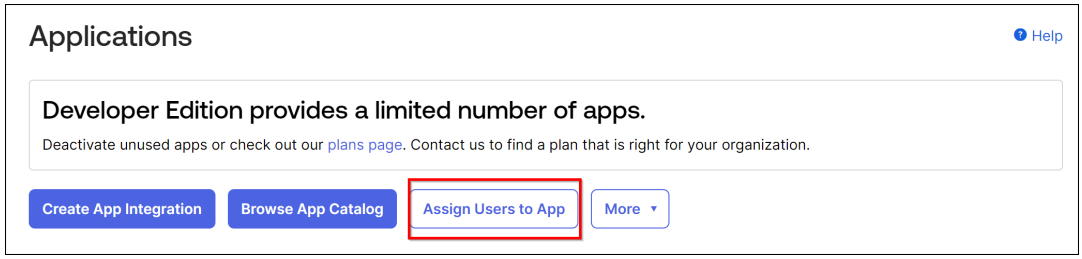
e) 单击“分配”，然后选择“保存并返回”。

f) 单击 **Done**（完成）。

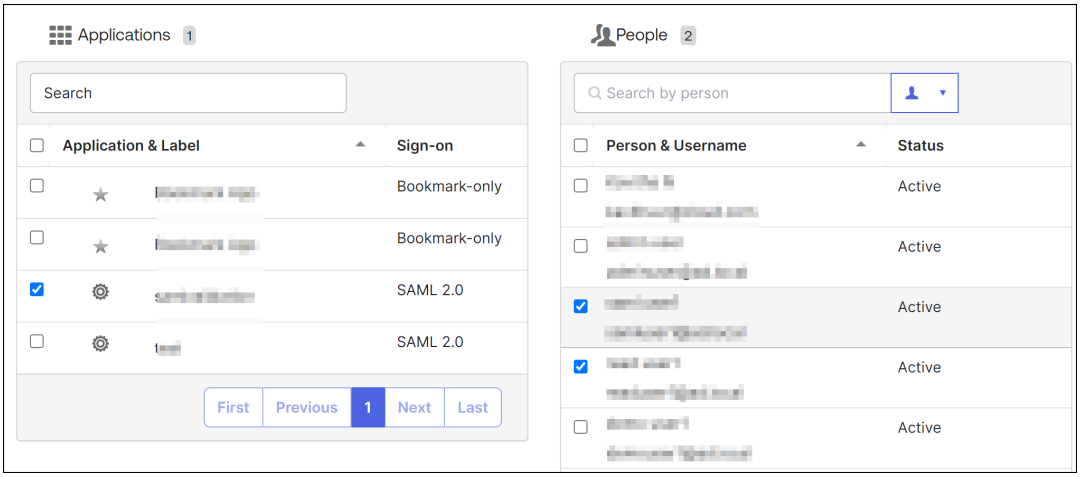
方法 **2**：

a) 导航到“应用程序”**>**“应用程序”。

b) 单击“向应用程序分配用户”。



c) 选择应用程序和用户，然后单击“下一步”。



d) 单击“确认分配”。

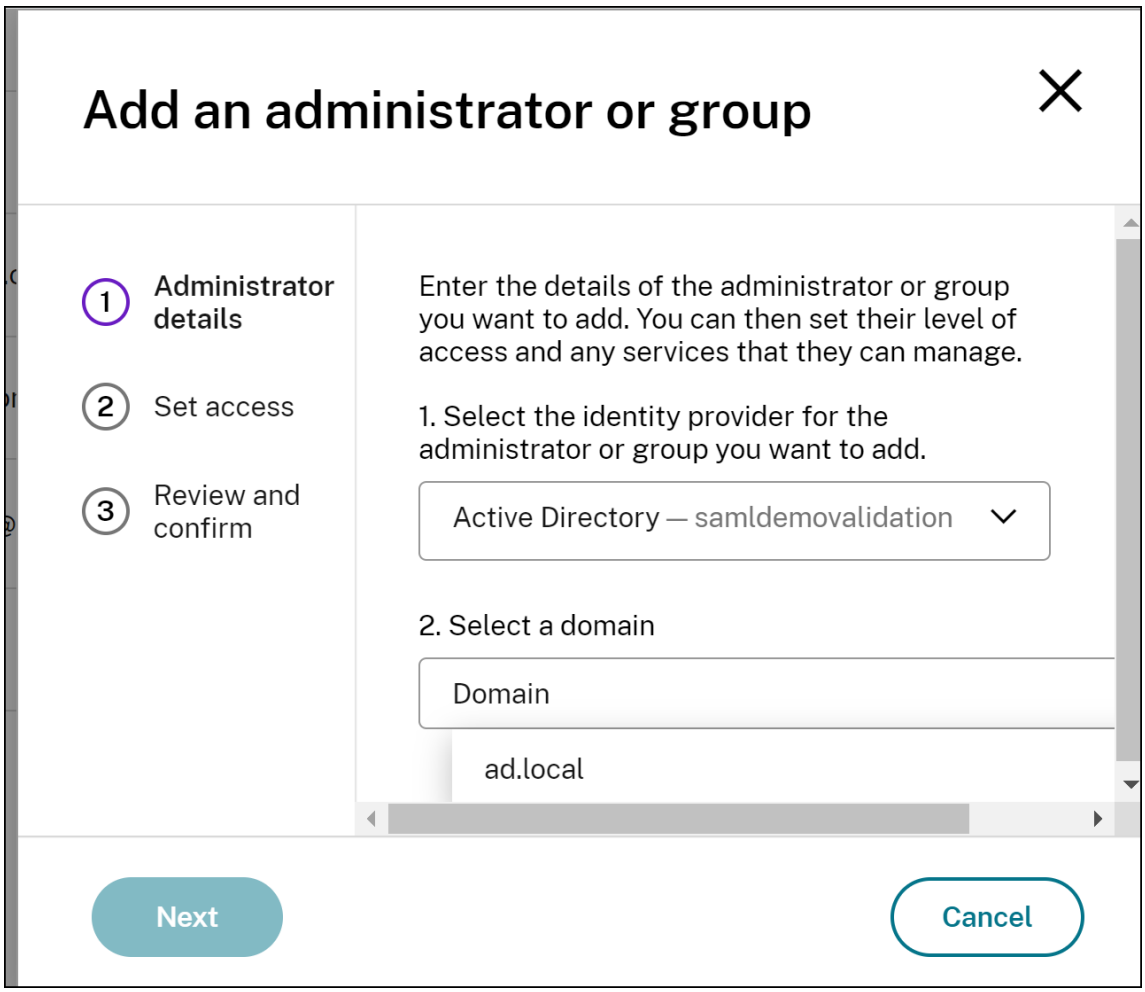
方法 **3**:

a) 导航到“目录” **>** “人员”。

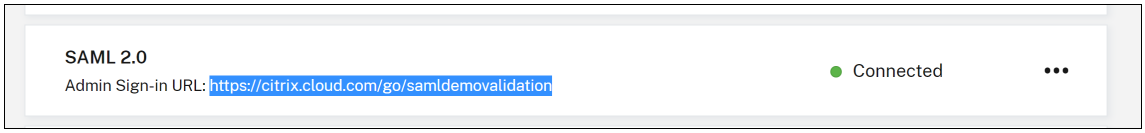
b) 选择任意用户。

c) 单击“分配应用程序”，将 SAML 应用程序分配给用户。

19. 分配用户后，登录 Citrix Cloud。
20. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
21. 在“管理员”选项卡中，单击“添加管理员/组”。
22. 从列表中选择 **Active Directory - [**您的 **SAML** 应用程序名称**]**，选择域，然后单击“下一步”。



23. 指定访问权限。
24. 检查一切是否正确，然后单击“发送邀请”。
25. 在“身份验证”选项卡中，您可以查看 SAML 2.0 的登录 URL。以下是该命令的一个示例：



系统要求

July 17, 2024

在开始使用 NetScaler 控制台之前，必须查看软件要求、浏览器要求、端口信息、许可信息和限制。

支持的浏览器

要访问 NetScaler 控制台，您的工作站必须支持网络浏览器。

支持以下浏览器。

Web 浏览器	版本
Microsoft Edge	79 及更高版本
Google Chrome	51 及更高版本
Safari	10 及更高版本
Mozilla Firefox	52 及更高版本

代理安装要求

在您的网络环境中安装和配置代理，以启用 NetScaler 控制台与数据中心中的托管实例之间的通信。在本地数据中心中，可以在 Citrix XenServer、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 服务器上安装代理。

代理要求是虚拟机管理程序必须为每个代理提供的虚拟计算资源。下表列出了使用所有 NetScaler 控制台功能的代理要求：

组件	要求
RAM	32 GB
虚拟 CPU	8
存储空间	30 GB
虚拟网络接口	1
吞吐量	1 Gbps

代理要求仅使用共用许可功能，请参阅池化 许可的轻量代理。

您还可以在 Microsoft Azure 或 AWS 或 Google Cloud 上安装代理。Citrix 建议您使用相应云市场中的以下虚拟机类型来使用 NetScaler 控制台的所有功能：

云	代理商要求	首选虚拟机类型
AWS	8 个虚拟 CPU、32 GB RAM 和 30 GB 存储空间	`m4.2xlarge`

云	代理商要求	首选虚拟机类型
Microsoft Azure	8 个虚拟 CPU、32 GB RAM 和 30 GB 存储空间	`Standard_D8s_v3`
Google Cloud	8 个虚拟 CPU、32 GB RAM 和 30 GB 存储空间	`e2-standard-8`

> 备注：
>
> 在 2024 年 7 月 23 日之后，Azure 将不再支持扩展基本安装程序版本 13.0 和 13.1 的代理。
>
> 对于 NetScaler 代理：
>
> - 具有 8 个虚拟 CPU、32 GB RAM 和 30 GB 存储空间的 NetScaler 代理不受影响。这些代理可以在没有任何中断的情况下进行升级。
> - 从 14.1 版开始的部署也不会受到影响。
>
> 对于轻量级代理：
>
> - 使用基本安装程序版本 13.0 或 13.1，拥有 4 个虚拟 CPU、8 GB RAM 和 30 GB 存储空间的轻量级代理在弃用日期之后无法向上扩展（增加 CPU 或 RAM）。
> - 要在将来扩展轻量级代理，请使用最新版本重新配置新代理。

有关安装代理的说明，请参阅以下链接：

- 在 Microsoft Azure 云上安装代理。
- 在 AWS上安装代理。
- 在 Google Cloud上安装代理。

用于池许可的轻量级代理

如果您计划仅将 NetScaler 控制台用于池化许可，则可以使用规格较低的代理，如下表所示：

组件	要求
RAM	8 GB
虚拟 CPU	4
存储空间	30 GB

只有 NetScaler 控制台支持规格较低（轻量级）的此类代理。

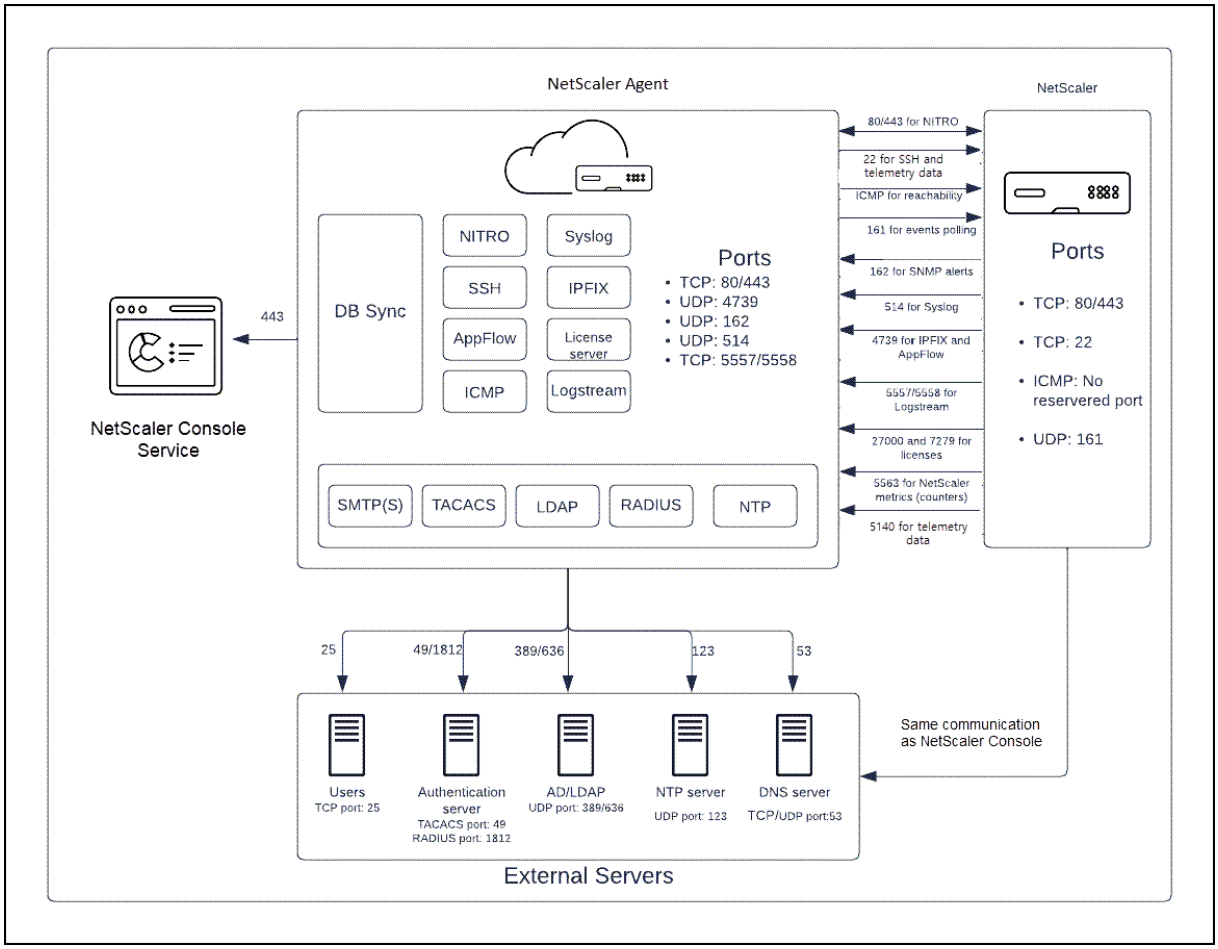
Citrix 建议您使用来自各自云市场的以下虚拟机类型仅使用池许可功能：

云	代理商要求	首选虚拟机类型
AWS	4 个虚拟 CPU、8 GB RAM 和 30 GB 存储空间	`m4.xlarge`。此实例类型提供 4 个虚拟 CPU、16 GB RAM 和 30 GB 存储空间。Citrix 建议使用此实例类型，因为它符合现有实例类型之间的大多数代理要求。
Microsoft Azure	4 个虚拟 CPU、8 GB RAM 和 30 GB 存储空间	`Standard_F4s_v2`
Google Cloud	4 个虚拟 CPU、8 GB RAM 和 30 GB 存储空间	`e2-standard-4`

> 注意
>
> 必须通过导航到“设置”>“全局设置”>“可配置功能”来禁用默认调度作业。

支持的端口

要在 NetScaler 实例和代理之间进行通信，请打开所需的端口。



NetScaler 代理的端口

此表说明了必须在代理上打开的所需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 NetScaler 控制台服务到 NetScaler 的 NITRO 通信。	NetScaler 代理到 NetScaler 和 NetScaler 到 NetScaler 代理
4739	UDP	用于从 NetScaler 到 NetScaler 控制台服务的 AppFlow 通信。	NetScaler 到 NetScaler 代理
162	UDP	从 NetScaler 实例向 NetScaler 控制台服务接收 SNMP 事件。	NetScaler 到 NetScaler 代理

端口	类型	详细信息	通信方向
514	UDP	从 NetScaler 实例向 NetScaler 控制台服务接收系统日志消息。	NetScaler 到 NetScaler 代理
5563	TCP	此端口是运行 NetScaler 控制台收集器服务所必需的。从 NetScaler 实例向 NetScaler 控制台接收 NetScaler 指标（计数器）。	NetScaler 到 NetScaler 控制台
5557/5558	TCP	用于从 NetScaler 到 NetScaler 控制台服务的 Logstream 通信（针对 WAF 安全违规、Web Insight 和 HDX Insight）。	NetScaler 到 NetScaler 代理
27000 和 7279	TCP	用于在 NetScaler 代理和 NetScaler 实例之间进行通信的许可端口。这些端口还用于 NetScaler 池许可。	NetScaler 到 NetScaler 代理
443	TCP	用于 NetScaler 代理和 NetScaler 控制台服务之间的通信端口	NetScaler 代理到 NetScaler 控制台服务
5140	UDP	接收 NetScaler Gateway 遥测数据的端口	NetScaler 到 NetScaler 控制台

NetScaler 实例的端口

下表说明了必须在 NetScaler 实例上打开的必需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 NetScaler 控制台到 NetScaler 实例的 NITRO 通信。	NetScaler 代理到 NetScaler 和 NetScaler 到 NetScaler 代理
22	TCP	用于代理和 NetScaler 之间的 SSH 通信。注意：此端口还用于 NetScaler 遥测。	NetScaler 代理到 NetScaler

端口	类型	详细信息	通信方向
无保留的端口	ICMP	检测 NetScaler 代理和 NetScaler 实例之间的网络可访问性。	NetScaler 代理到 NetScaler
161	UDP	轮询来自 NetScaler 实例的事件。	NetScaler 代理到 NetScaler

NetScaler 内置代理的端口

下表说明了 NetScaler 内置代理必须具备的所需端口。

端口	类型	详细信息	通信方向
443	TCP	用于从 NetScaler 控制台到 NetScaler 实例的 NITRO 通信。	NetScaler 控制台到 NetScaler 内置代理和 NetScaler 内置代理到 NetScaler 控制台

> 注
>
> 意 NetScaler 控制台服务的端点与尝试注册代理时生成的“服务 URL”相同。该代理使用服务 URL 来定位 NetScaler 控制台。

确保允许访问以下端点 URL：

- 下载服务：

```
https://download.citrixnetworkapi.net
```

- 信托服务：

```
*.citrixnetworkapi.net
```

- 服务 URL：

```
*.agent.adm.cloud.com
*.adm.cloud.com
adm.cloud.com
```

- Citrix Cloud 连接：

```
citrix.cloud.com
accounts.cloud.com
```


弃用的 **FQDN**

在以下 NetScaler 控制台的使用中，不推荐使用某些 FQDN。为了帮助您在没有任何中断的情况下切换到新的 FQDN，已弃用的 FQDN 将继续工作一段时间，并将逐步淘汰。

NetScaler 控制台终端节点	旧的 FQDN	新 FQDN
NetScaler 控制台用户界面访问权限	netscalermas.cloud.com	adm.cloud.com
服务 URL	agent.netscalermgmt.net	*.agent.adm.cloud.com 注意：* 的值将取决于您的数据可用的 PoP（接入点）。
API 交互	netscalermas.cloud.com	api.adm.cloud.com

所需的 **NetScaler** 最低版本

> 注意
>
> NetScaler 10.5、11.0 和 12.0 版本已达到寿命终结 (EOL)。有关更多信息，请参阅 产品列表。推荐的 NetScaler 版本为 12.1。

NetScaler 控制台功能	NetScaler 软件版本
样书	10.5 及更高版本
使用 Jobs 进行监视/报告和配置	10.5 及更高版本
分析	
HDX Insight	10.1 及更高版本
Gateway Insight	11.0.65.31 及更高版本
Security Insight	11.0.65.31 及更高版本

NetScaler 控制台分析解决方案的要求

所需的最低 **Citrix Virtual Apps and Desktops** 版本

NetScaler 控制台功能	Citrix Virtual Apps and Desktops 版本
HDX Insight	Citrix Virtual Apps and Desktops 7.0 及更高版本

> 注意
>
> NetScaler Gateway 功能（在版本 9.3 和 10.x 中标记为接入网关企业版）必须在 NetScaler 实例上可用。NetScaler 控制台不支持独立的 Access Gateway 标准设备。

NetScaler 控制台可以为在 Citrix 虚拟应用程序或桌面上发布并通过 Citrix Workspace 访问的应用程序生成报告。但是，此功能取决于安装 Citrix Workspace 的操作系统。目前，NetScaler 不解析通过在 iOS 或 Android 操作系统上运行的 Citrix Workspace 访问的应用程序或桌面的 ICA 流量。

HDX Insight 支持的瘦客户端

NetScaler 控制台支持以下瘦客户端来监视在软件版本 11.0 Build 65.31 及更高版本上运行的 NetScaler 实例：

- 基于 Dell Wyse Windows 的瘦客户端
- 基于 Dell Wyse Linux 的瘦客户端
- Dell Wyse ThinOS 的瘦客户端
- 基于 10ZiG Ubuntu 的瘦客户端

HDX Insight 需要 **NetScaler** 实例许可证

适用于 HDX Insight 的 NetScaler 控制台收集的数据取决于受监视的 NetScaler 实例的版本和安装的许可。HDX Insight 报告仅显示在软件版本 10.5 及更高版本上运行的 NetScaler Premium 和企业设备。

NetScaler 许可证/持续时间	5 分钟	1 小时	1 天	1 周	1 个月
Standard	否	否	否	否	否
高级	是	是	否	否	否
Premium	是	是	是	是	是

支持的操作系统和 **Citrix Workspace** 版本

下表列出了 NetScaler 控制台支持的操作系统，以及每个系统目前支持的 Citrix Workspace 版本：

操作系统	Citrix Workspace 版本
Windows	4.0 标准版
Linux	13.0.265571 及更高版本
Mac	11.8 (Build 238301) 及更高版本
HTML5	1.5
Chrome 应用程序	1.5

许可证

March 10, 2024

从 NetScaler 控制台服务版本 14.1-21.x 开始，许可的 VIP 概念被移除。现在，NetScaler 控制台服务中提供了无限数量的 VIP。您不再需要购买 NetScaler 控制台虚拟服务器许可，因为 VIP 许可 SKU 将很快变为终止销售 (EOS) 和续订结束 (EOR)。

对 NetScaler 控制台服务存储的更改如下：

- NetScaler 控制台服务存储 SKU 将很快终止销售 (EOS) 和续订结束 (EOR)。
- 现在，默认 NetScaler 控制台服务存储权限为 5GB。
- 过去购买的任何 NetScaler 控制台服务存储将在期限结束之前兑现。
- 过去购买的任何 NetScaler 控制台 VIP 许可证，只要您有权按比例获得 NetScaler 控制台服务存储，则在期限结束前均可兑现。
- 如果您购买了其他套餐以使您有权获得更高的 NetScaler 控制台存储权限，则默认 5GB 将更改为与授权相匹配。

> 注意：
>
> 如果您之前购买了虚拟服务器，则在订阅期结束之前，每台虚拟服务器适用 500 MB 的存储空间。

NetScaler 控制台功能需要 **NetScaler** 许可

下表列出了使用某些 NetScaler 控制台功能所需的 NetScaler 许可。

NetScaler 控制台功能组	NetScaler 控制台功能	NetScaler 和网关许可证要求
分析	HDX Insight	Advanced（报告 < 1 小时） Premium（报告 = 无限制）

NetScaler 控制台功能组	NetScaler 控制台功能	NetScaler 和网关许可证要求
分析	Security Insight	使用 App Firewall 许可证的 Premium（或）Advanced
分析	Gateway Insight	Advanced（报告 < 1 小时） Premium（报告 = 无限制）
应用程序	应用程序统计信息（应用程序控制板、应用程序安全性控制板）	应用程序控制板和应用程序安全控制板上的 NetScaler Web App Firewall 相关信息需要带有应用程序防火墙许可证的高级版（或）高级版
应用程序	API 网关	高级（或）高级许可
应用程序	样书	不适用
应用程序	库存管理-基础设施控制面板、实例组、实例控制板和站点	不适用
应用程序	事件管理和系统日志	不适用
应用程序	配置作业、配置审核和配置建议	不适用
应用程序	网络报告（实例级别）	不适用
应用程序	网络报告（虚拟服务器级别）	不适用
应用程序	网络功能（虚拟服务器、服务、服务组、服务器的清晰可见性和管理）	不适用
应用程序	SSL 证书管理（实例级别）	不适用
应用程序	SSL 证书管理（虚拟服务器级别）	不适用
系统	RBAC 和外部身份验证（实例级）	不适用
系统	RBAC 和外部身份验证（虚拟服务器级别）	不适用

查看虚拟服务器订阅的到期检查

您可以在 NetScaler 控制台中查看已安装许可的状态以及许可的到期时间和允许的存储限制。

查看许可证的状态：

1. 导航到 帐户 > 订阅。
2. 在 权利 部分中，您可以查看许可虚拟服务器的详细信息以及到期天数：
    - 授权的虚拟服务器：可供许可的虚拟服务器数量。
    - 授权的第三方虚拟服务器：您可以使用许可证管理的第三方虚拟服务器的数量。

- 授权存储：许可证的存储限制。
- 到期天数：许可证到期前剩余的天数。

查看虚拟服务器上启用的分析类型

在所选虚拟服务器上启用 AppFlow 后，可以从“订阅”页面查看在许可的虚拟服务器或第三方虚拟服务器上启用的分析类型。

1. 导航到 帐户 **>** 订阅。
2. 在“虚拟服务器分析摘要”部分中，选择许可虚拟服务器的类型。
3. 许可的虚拟服务器页面显示已许可的虚拟服务器列表。在此页面上，分析状态 列显示在虚拟服务器上启用的分析类型。

升级公告

January 29, 2024

作为网络管理员，您可以在 NetScaler 控制台中管理许多在不同 NetScaler 版本上运行的 NetScaler 实例。监视每个 NetScaler 实例的生命周期可能是一项繁琐的任务。您必须访问 NetScaler 产品矩阵，确定即将或达到生命周期终止 (EOL) 或维护终止 (EOM) 的 NetScaler 实例。然后，计划他们的升级。

为了简化此过程，NetScaler 控制台升级公告可通过以下方式帮助您监视 NetScaler 实例的生命周期：

- 识别达到或到达 EOL 或 EOM 的实例。因此，您可以在 EOL 或 EOM 日期之前规划 NetScaler 升级。
- 突出显示不在最新版本或内部版本上的实例。您可以将这些实例升级到最新版本或构建。通过此升级，您将收到有关新功能和已修复问题的更新。
- 突出显示不在首选 NetScaler 版本中的实例。一些组织可能为其实例提供首选的 NetScaler 版本。在 NetScaler 控制台中，您可以根据构建稳定性、功能和其他注意事项为组织设置首选 版本。然后，查看并升级不在首选构建上的实例。运行首选构建的实例以星形图标标示。
- 突出显示在最受欢迎的版本或版本上运行的实例。运行常用版本的实例以功能区图标标示。

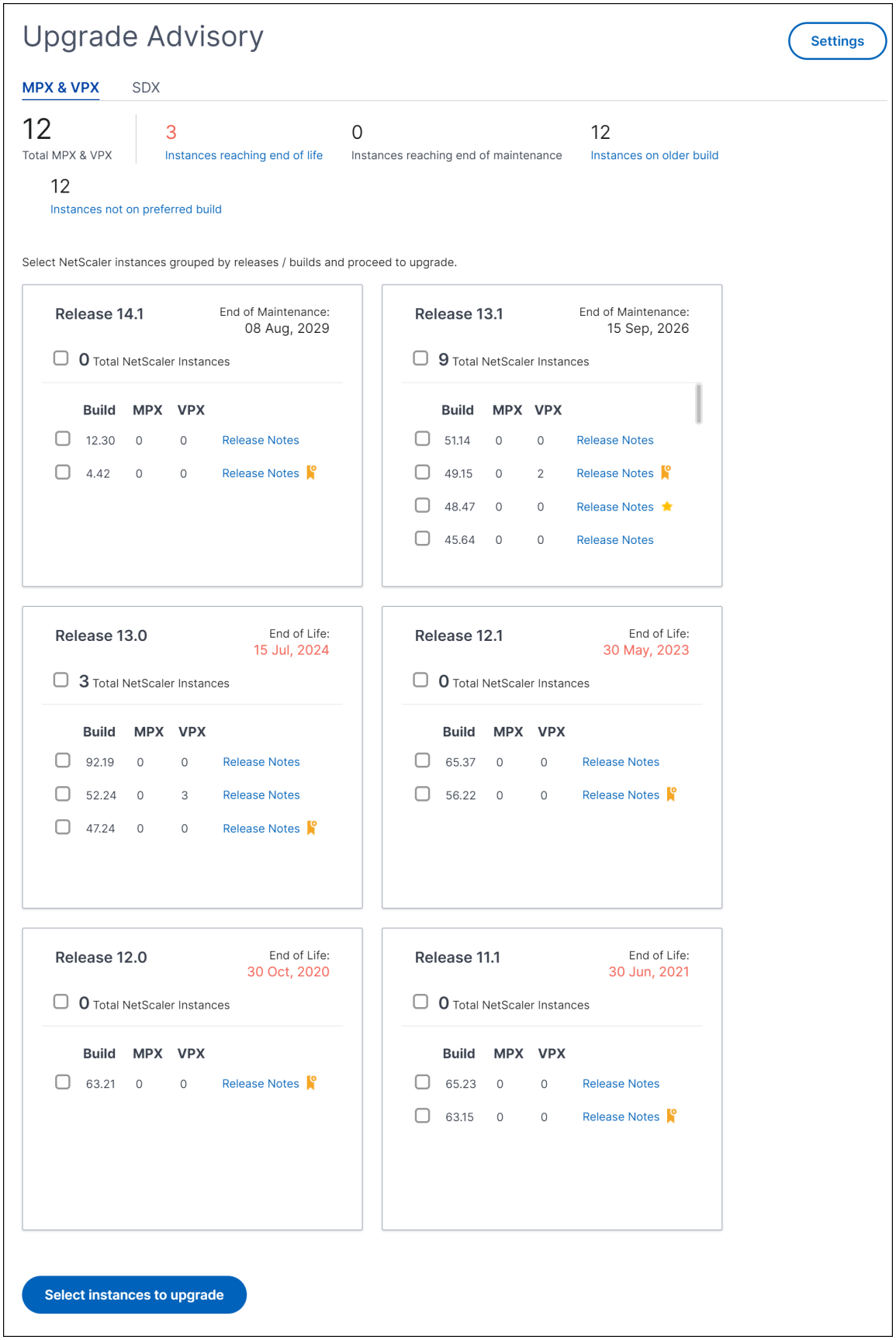
升级公告提供了指向相应发行说明的链接。利用这些信息，您可以查看和决定要升级的 NetScaler 版本。您可以从“升级公告”页面继续创建维护任务以升级 NetScaler 实例。

> 重要
>
> 升级公告仅监视 NetScaler 软件版本的 EOL。它不检查 NetScaler 设备的 EOL。

查看升级公告

导航 基础结构 **>** 实例公告 **>** 升级建议 并查看以下信息：

- NetScaler 实例的总数。
- 实例即将结束。
- 维护即将结束的实例。
- 旧版本中的实例。
- 不在首选构建中的实例。
- 各种 NetScaler 版本的生命周期结束和维护终止日期。

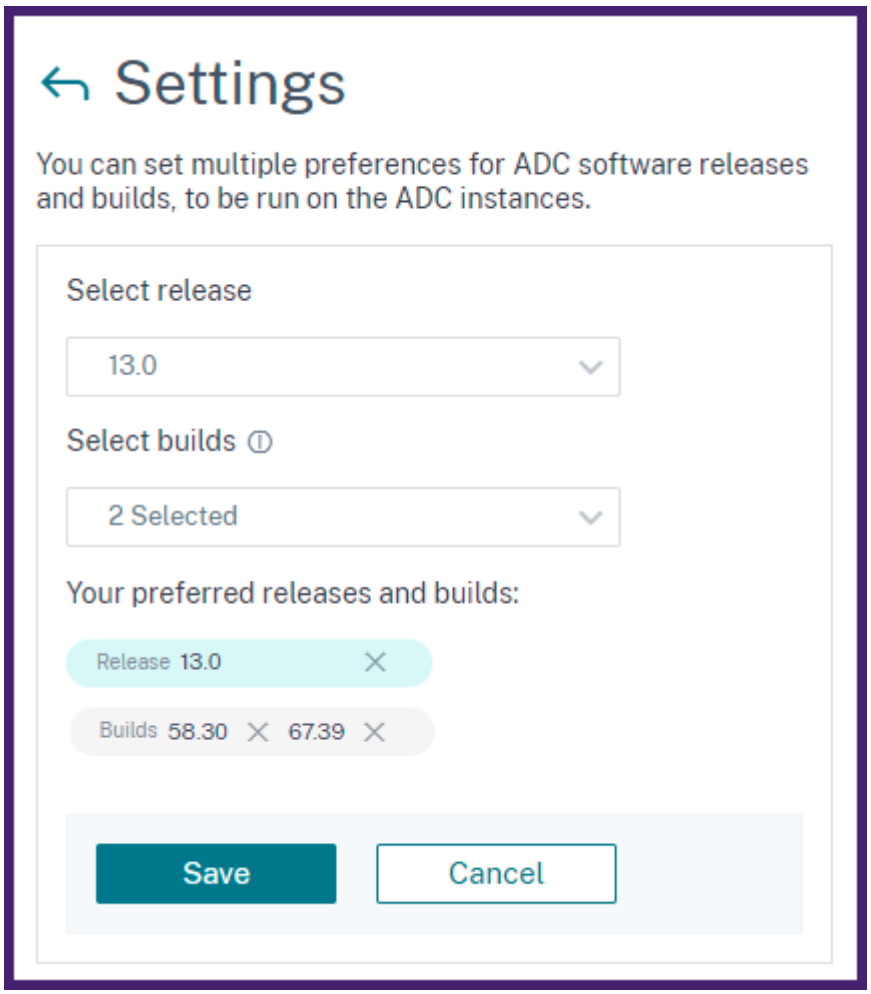


升级公告页面按版本 对 NetScaler 实例进行分组。发行说明 链接引导您查看特定的 NetScaler 发行说明。在决定升级之前，请查看新功能、已修复问题和已知问题。您可以选择不同版本的多个 NetScaler 实例进行一次升级。继续升级时，它会创建升级作业。参见，升级 NetScaler 实例。

设置首选构建

作为管理员，您可以为组织定义首选的 NetScaler 版本。执行以下操作以设置首选构建：

1. 在 基础结构 **>** 实例公告 **>** 升级建议中，单击 设置。
2. 选择首选的版本和版本。



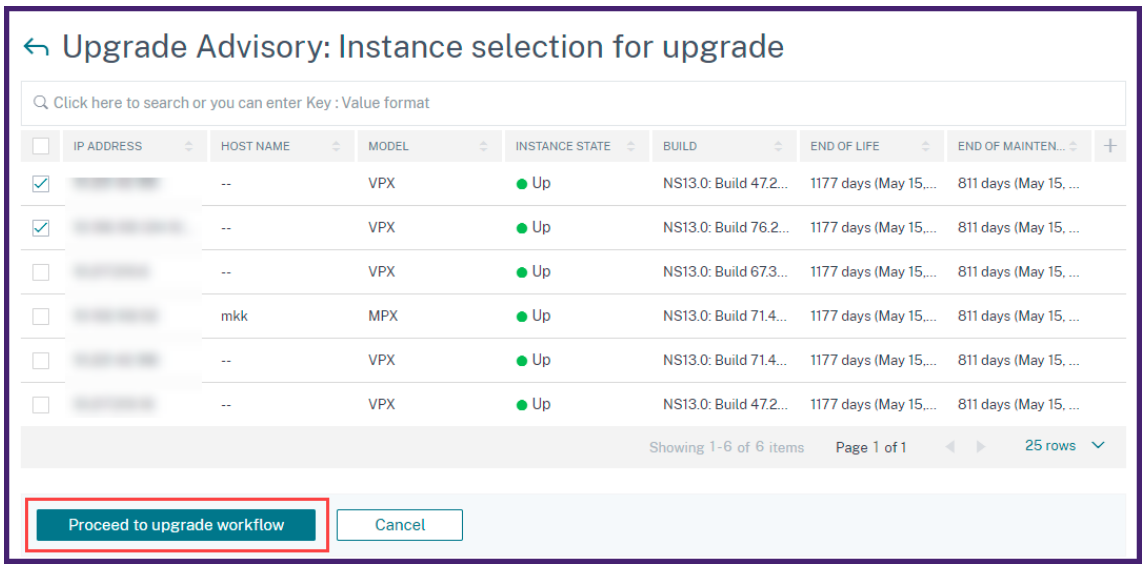
在此示例中，首选的构建是 `13.0-58.30` 和 `13.0-67.39`。

3. 单击保存。

升级 **NetScaler** 实例

在 升级公告 页面中，查看后，执行以下步骤来升级所需的 NetScaler 实例：

1. 选择要升级的实例构建，然后单击 选择要升级的实例。
2. 选择要升级的 NetScaler 实例，然后 单击“继续升级工作流程”。



此工作流创建升级作业。

3. 在“选择实例”选项卡中，

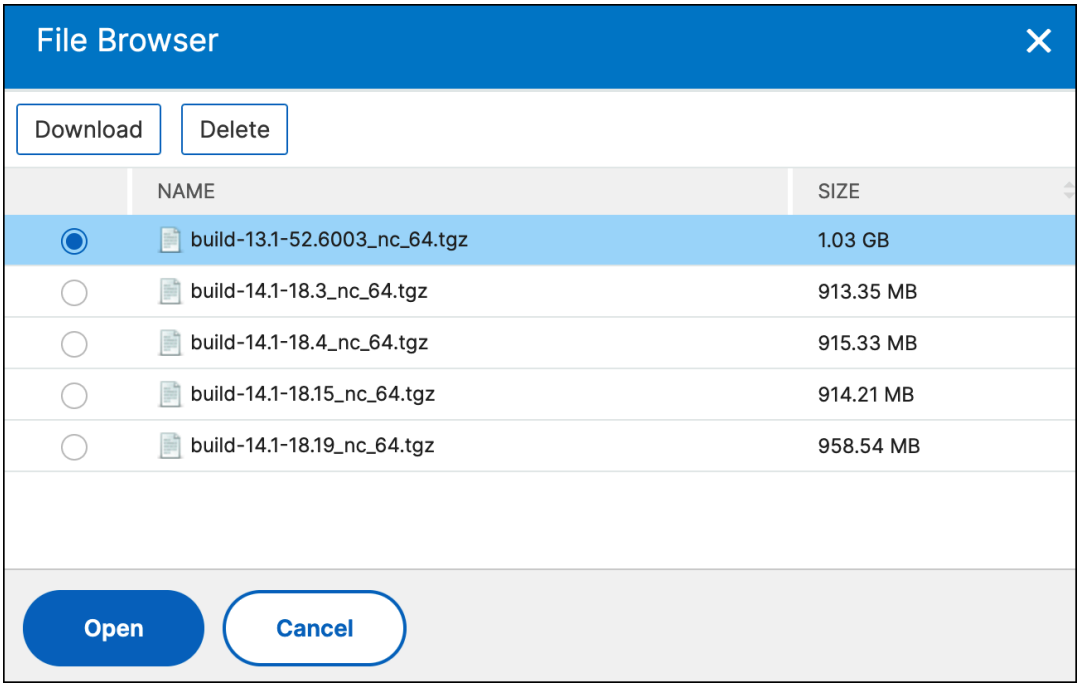
   a) 为升级作业指定名称。

   b)（可选）如果要添加其他实例，请单击 添加实例。

   c) 单击下一步。

4. 在“选择映像”标签中，从映像库或本地或设备中选择 NetScaler 镜像。

   - 从映像库中选择：从列表中选择 NetScaler 镜像。此选项列出了 NetScaler 下载网站上提供的所有 NetScaler 镜像。



NetScaler 软件映像显示带有星形图标的首选版本。此外，大多数下载的版本都带有书签图标。

- 从本地或设备中选择：您可以从本地电脑或 NetScaler 设备上载图像。当您选择 NetScaler 设备时，NetScaler 控制台 GUI 会显示 `/var/mps/mps_images` 中存在的实例文件。从 NetScaler 控制台 GUI 中选择镜像。
- 如果所选图像已经可用，则跳过将图像上载到 **NetScaler** -此选项检查所选图像在 NetScaler 中是否可用。升级任务会跳过上载新映像，而使用 NetScaler 中可用的映像。
- 成功升级后从 **NetScaler** 清理软件映像 - 此选项将在实例升级后清除 NetScaler 实例中上载的映像。

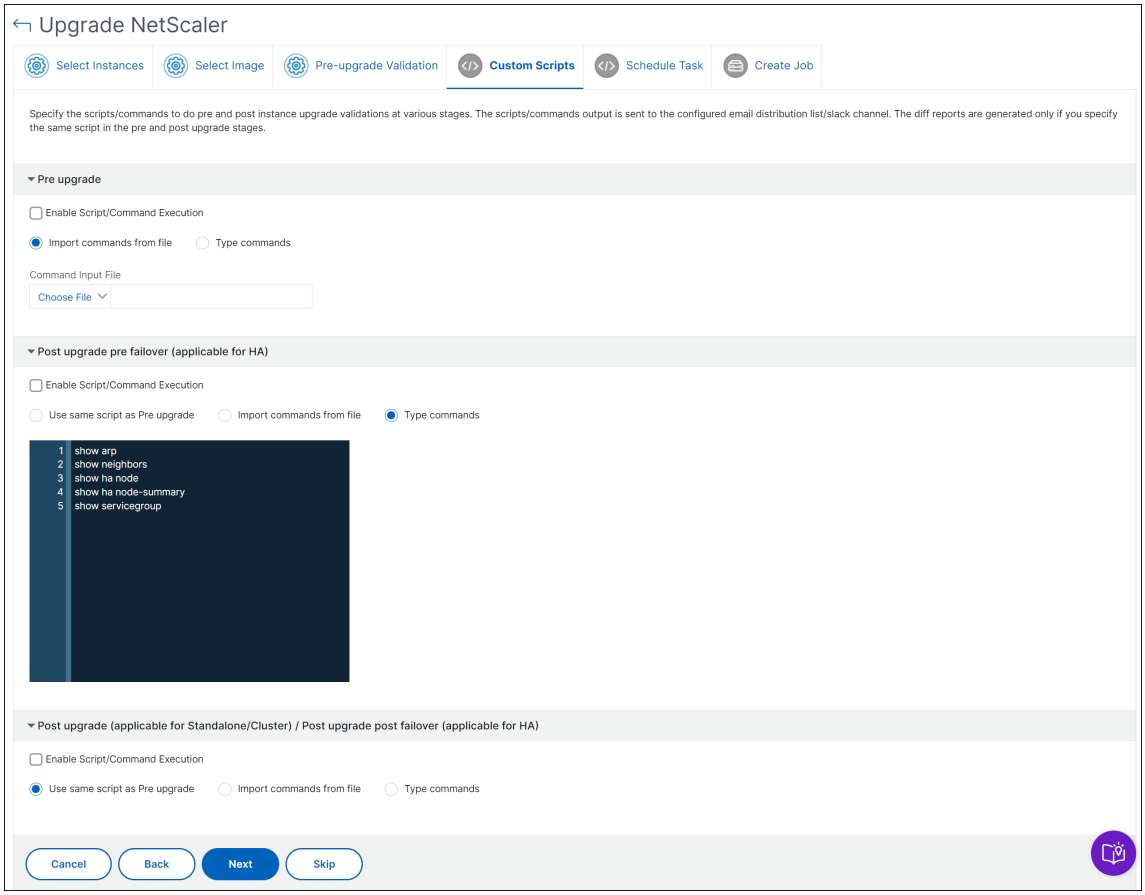
单击 下一步 开始对所选实例进行升级前验证。

5. 升级前验证 选项卡显示失败的实例。您可以删除失败的实例，然后单击 下一步。

   - 磁盘空间检查：如果您遇到实例上磁盘空间不足的问题，可以检查并清理磁盘空间。请参阅清理 NetScaler 磁盘空间。
   - 策略检查：如果 NetScaler 控制台发现不支持的经典策略，您可以删除此类策略以创建升级任务。

   > 注意：
   >
   > 如果您指定群集 IP 地址，则 NetScaler 控制台仅在指定的实例上进行升级前验证，不在其他群集节点上进行升级前验证。

6. 可选，在 自定义脚本 选项卡中，指定要在实例升级之前和之后运行的脚本。

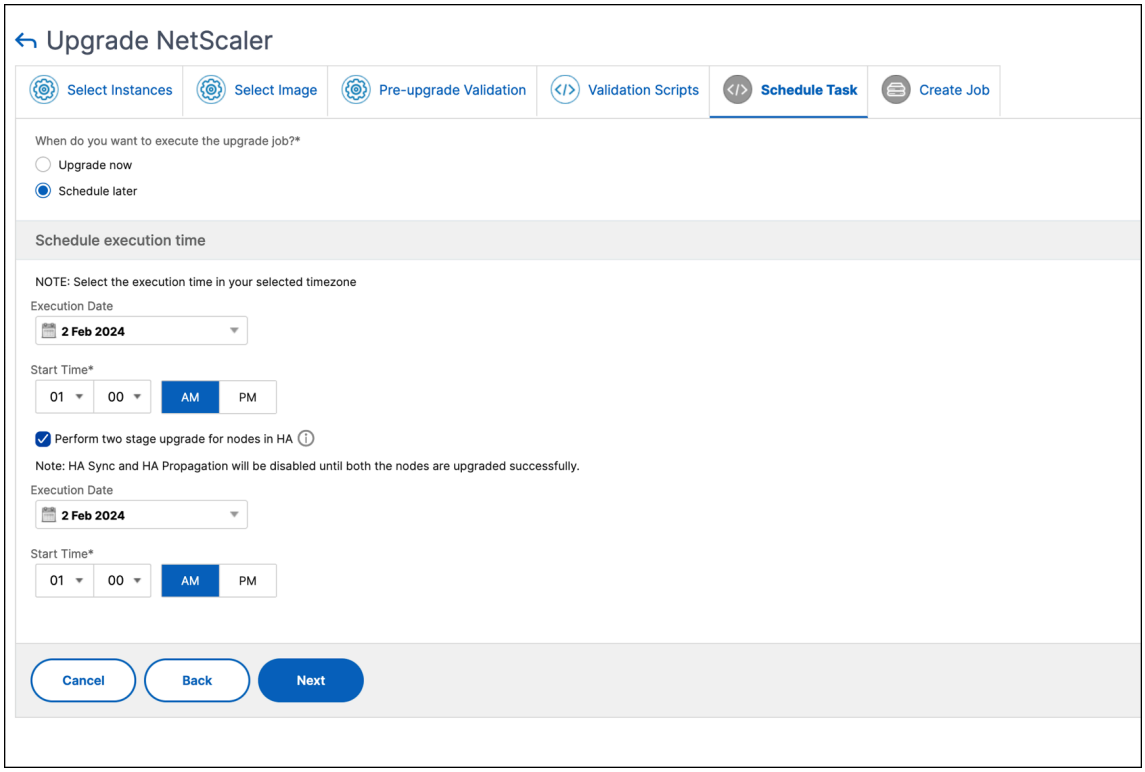


有关更多信息，请参阅 使用自定义脚本。

7. 在计 划任务中，选择以下选项之一：

   - 立即升级 -升级作业将立即运行。
   - 稍后计划 -选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。

   如果要分两个阶段升级 NetScaler 高可用性对，请选择“为 HA 中的节点执行两阶段升级”。



有关更多信息，请参见 升级 NetScaler 高可用性对。

8. 在“创建作业”选项卡中，指定以下详细信息：

   如果您安排升级作业，则可以指定要将映像上载到实例的时间：

   - 立即上载：选择此选项可立即上载图片。但是，升级作业将在计划的时间运行。
   - 执行时上载：选择此选项可在升级任务执行时上载映像。

有关其他选项的更多信息，请参见 NetScaler 升级选项。

安全公告

January 29, 2024

安全、可靠且具有弹性的基础设施是任何组织的生命线。NetScaler 控制台安全公告亮点：

- 常见漏洞和暴露 **(CVE)** 检测和修复 -使您能够识别使 NetScaler 实例面临风险的 CVE 并提出补救建议。
- 文件完整性监视 -使您能够确定是否对 NetScaler 构建文件进行了任何更改或添加。

作为管理员，您必须确保：

- 跟踪任何新的常见漏洞和暴露 (CVE)，评估 CVE 的影响，了解补救措施并解决漏洞。

- 检查 NetScaler 编译文件的完整性。

安全公告功能

以下安全公告功能可帮助您保护基础结构。

CVE：

功能	说明
系统扫描	默认情况下，每周扫描一次所有托管实例。NetScaler 控制台决定系统扫描的日期和时间，您无法对其进行更改。
按需扫描	需要时，您可以手动扫描实例。如果上次系统扫描后经过的时间很长，则可以运行按需扫描以评估当前的安全状态。或者在应用补救措施后进行扫描，以评估修改后的状态。
CVE 影响分析	显示影响您的基础设施的所有 CVE 的结果以及所有 NetScaler 实例受到影响的结果，并提出补救建议。使用此信息应用补救措施来修复安全风险。
CVE 报告	存储最近五次扫描的副本。您可以下载 CSV 格式的这些报告并对其进行分析。
CVE 存储库	详细介绍了 Citrix 自 2019 年 12 月以来宣布的所有与 NetScaler 相关的 CVE，这可能会影响您的 NetScaler 基础架构。您可以使用此视图来了解安全公告范围中的 CVE，并了解有关 CVE 的更多信息。有关不支持的 CVE 的信息，请参阅 安全公告中不支持的 CVE。

文件完整性监视：

功能	说明
按需扫描	必须运行按需扫描，才能获得 NetScaler 构建文件中检测到的任何文件更改的结果。
文件完整性监视扫描	将当前 NetScaler 构建文件的二进制哈希值与原始二进制哈希值进行比较，并突出显示是否有任何文件更改或文件添加。您可以在“文件完整性监视”选项卡下查看扫描结果。

注意事项

- Security Advisory 不支持已到达生命周期已结束 (EOL) 状态的 NetScaler 版本。我们建议您升级到 NetScaler 支持的内部版本或版本。

- CVE 检测支持的实例：所有 NetScaler（SDX、MPX、VPX）和 Gateway。
- 文件完整性监视支持的实例：MPX、VPX 实例和网关。
- 支持的 CVE：2019 年 12 月之后的所有 CVE。

  > 注意：
  >
  > NetScaler 控制台安全公告不支持检测和修复影响 Windows 版 NetScaler Gateway 插件的漏洞。有关不支持的 CVE 的信息，请参阅 安全公告中不支持的 CVE。

- 在识别漏洞时，NetScaler 控制台安全公告不考虑任何类型的功能配置错误。
- NetScaler 控制台安全公告仅支持识别和修复 CVE。它不支持识别和修复“安全”文章中强调的安全问题。
- NetScaler、Gateway 版本的范围：该功能仅限于主版本。安全公告在其范围内不包括任何特殊版本。
  - 管理员分区不支持安全公告。
- 以下类型的扫描可用于 CVE：
  - 版本扫描：此扫描需要 NetScaler 控制台将 NetScaler 实例的版本与可用修复程序的版本和内部版本进行比较。此版本比较有助于 NetScaler 控制台安全公告确定 NetScaler 是否容易受到 CVE 的攻击。例如，如果在 NetScaler 版本上修复 CVE 并构建 xx.yy，则安全公告会将版本低于 xx.yy 的所有 NetScaler 实例视为易受攻击。安全公告目前支持版本扫描。
  - 配置扫描：此扫描需要 NetScaler 控制台将特定于 CVE 扫描的模式与 NetScaler 配置文件 (nsconf) 进行匹配。如果 NetScaler ns.conf 文件中存在特定的配置模式，则认为该实例容易受到该 CVE 的影响。此扫描通常与版本扫描一起使用。
    安全公告目前支持配置扫描。
  - 定制扫描：此扫描需要 NetScaler 控制台连接托管的 NetScaler 实例，向其推送脚本并运行脚本。脚本输出有助于 NetScaler 控制台识别 NetScaler 是否容易受到 CVE 的攻击。示例包括特定的 shell 命令输出、特定的 CLI 命令输出、某些日志以及某些目录或文件的存在或内容。如果配置扫描无法解决相同问题，Security Advisory 还会使用自定义扫描来匹配多个配置模式。对于需要自定义扫描的 CVE，脚本会在每次运行预设或按需扫描时运行。有关收集的数据和特定自定义扫描选项的更多信息，请参阅该 CVE 的“安全公告”文档。
- 以下扫描可用于文件完整性监视：
  - 文件完整性监视扫描：此扫描需要 NetScaler 控制台连接托管的 NetScaler 实例。NetScaler 控制台通过在 NetScaler 中运行脚本并收集 NetScaler 编译文件的当前二进制哈希值来比较哈希值。比较后，NetScaler 控制台提供的结果包括修改的现有文件总数和新添加的文件总数。作为管理员，您可以联系您的组织数字取证，以进一步调查扫描结果。

    扫描以下文件：

    * /netscaler

    * /bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin
    * /lib, /libexec, /usr/lib, /usr/libexec, /usr/local/lib, /usr/lib32, /compat
    * /etc
    * 其余的 /usr
    * /root, /home, /mnt

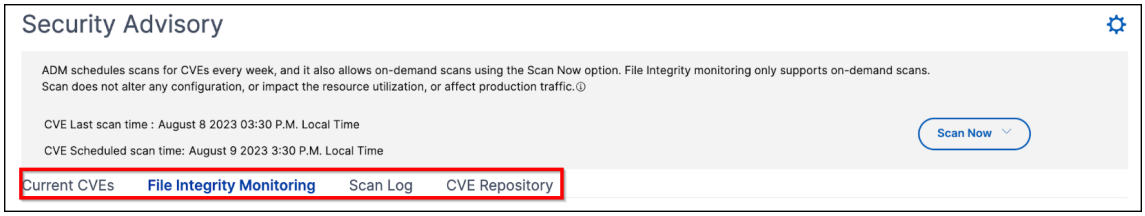
- 扫描不会影响 NetScaler 上的生产流量，也不会更改 NetScaler 上的任何 NetScaler 配置。
- NetScaler 控制台安全公告不支持 CVE 缓解措施。如果您已对 NetScaler 实例应用了缓解措施（临时变通方案），则在您完成修复之前，NetScaler 控制台仍会将 NetScaler 识别为易受攻击的 NetScaler。
- 对于 FIPS 实例，不支持 CVE 扫描，但支持文件完整性监视扫描。
- 有些文件更改可能是在设备正常运行过程中发生的，而另一些则可能需要进一步调查。在查看文件更改时，以下内容可能会有所帮助：
    - 使用脚本或插件可能会导致 /netscaler 目录（在 **.html** 和 **.js** 文件中）发生变化。
    - /etc 目录包含配置文件，这些文件可能会在启动系统后因意外干预而被更改。
    - 如果有，那就不寻常了：
        * /bin、/sbin 或 /lib 目录中的报告
        * /netscaler 目录中有新的.php 文件

如何使用安全公告控制板

要访问 安全公告 控制面板，请从 NetScaler 控制台 GUI 中导航到基础架构 **>** 实例公告 **>** 安全公告。

控制板包括四个选项卡：

- 当前的 CVE
- 文件完整性监视
- 扫描日志
- CVE 存储库



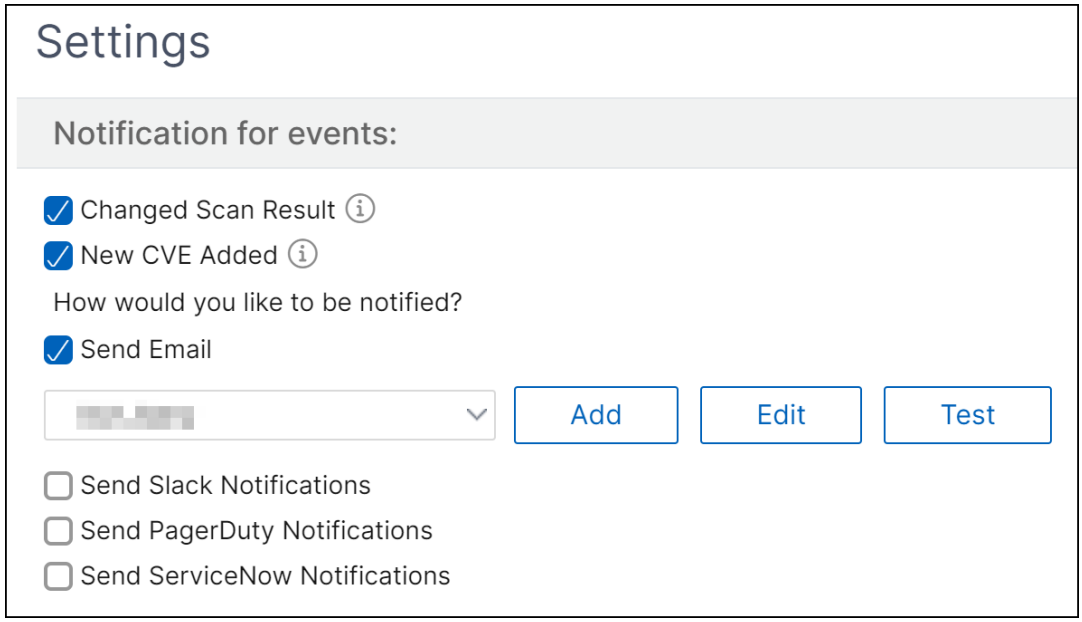
> 重要：
>
> 在 安全公告 GUI 或报告中，可能不会显示所有 CVE，您可能只能看到一个 CVE。解决方法是，单击“立即扫描” > “扫描 **CVE**”以运行按需扫描。扫描完成后，范围内的所有 CVE（大约 15 个）都将显示在 UI 或报告中。

控制板右上角是设置图标，它允许您：

- 启用和禁用通知（仅适用于 CVE 检测）。

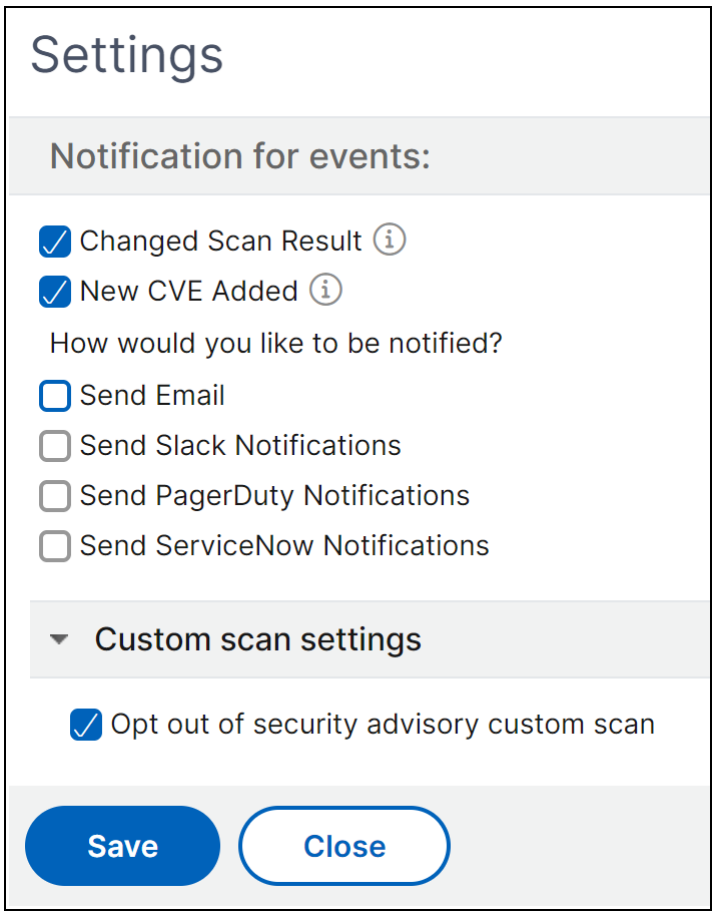
  您可以收到以下有关 CVE 影响的通知。

  - 发送电子邮件、Slack、PagerDuty 和 ServiceNow 通知，了解 CVE 扫描结果变更以及 CVE 存储库中添加的新 CVE。
  - CVE 影响扫描结果变更的云端通知。



- 配置自定义扫描设置（仅适用于 CVE）

  您可以单击“自定义扫描设置”列表以查看其他设置复选框。您可以选择复选框并选择退出这些 CVE 自定义扫描。安全公告中不会评估需要自定义扫描的 CVE 对您的 NetScaler 实例的影响。



当前的 **CVE**

此选项卡显示影响您的实例的 CVE 数量以及受 CVE 影响的实例。这些选项卡不是顺序的，作为管理员，您可以根据您的使用案例在这些选项卡之间切换。

显示影响 NetScaler 实例的 CVE 数量的表格包含以下详细信息。

CVE ID：影响实例的 CVE 的 ID。

发布日期：该 CVE 发布安全公告的日期。

严重性得分：严重性类型（高/中/严重）和得分。要查看得分，请将鼠标悬停在严重性类型上。

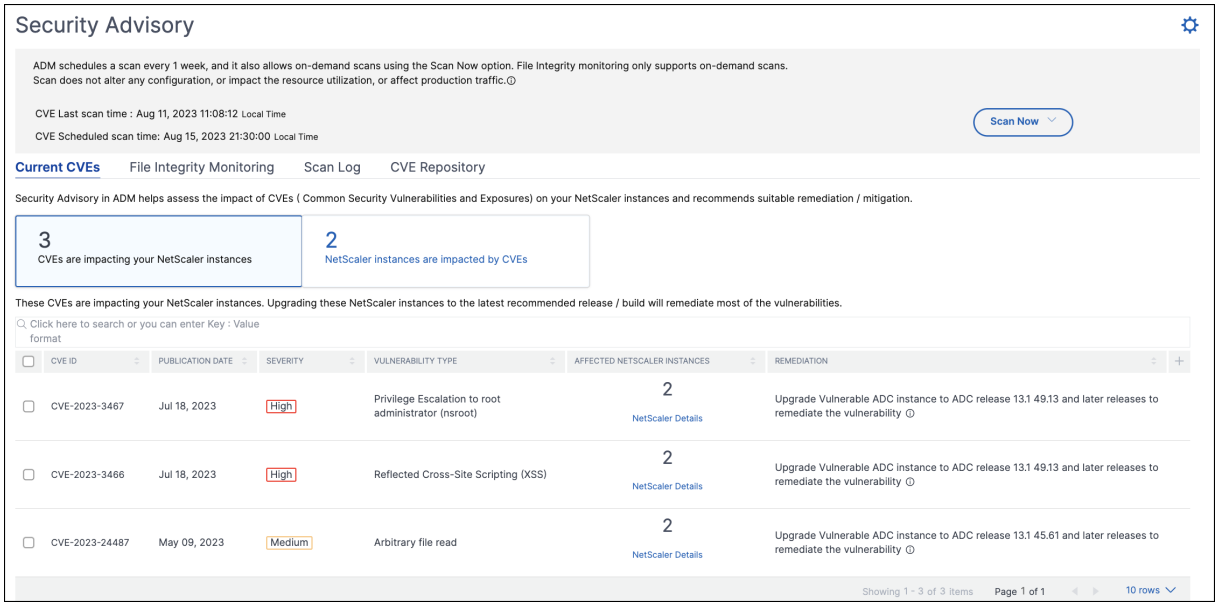
漏洞类型：此 CVE 的漏洞类型。

受影响的 **NetScaler** 实例：CVE ID 所影响的实例数。将鼠标悬停在上方时，将显示 NetScaler 实例列表。

补救措施：可用的补救措施，即升级实例（通常）或应用配置包。

同一实例可能受到多个 CVE 的影响。此表可帮助您查看一个特定 CVE 或多个选定 CVE 正在影响多少个实例。要查看受影响实例的 IP 地址，请将鼠标悬停在“受影响 **NetScaler** 实例”下的 NetScaler 详细信息上。要查看受影响实例的详细信息，请单击表底部的查 看受影响的实 例。
您还可以通过单击加号在表中添加或删除列。

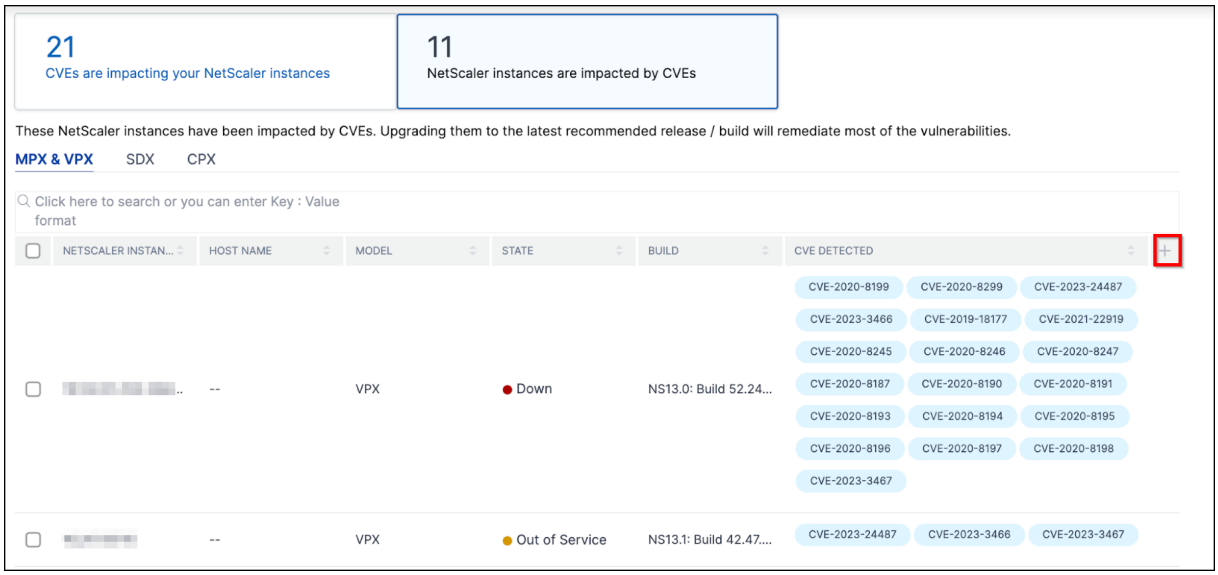
在此屏幕中，影响您的实例的 CVE 数量为 3 个，受这些 CVE 影响的实例数量为两个。



<number of>NetScaler 实例受 CVE 影响标签向您显示所有受影响的 NetScaler 控制台 NetScaler 实例。该表显示了以下详细信息：

- NetScaler IP 地址
- 主机名
- NetScaler 型号
- NetScaler 的状态
- 软件版本和构建
- 影响 NetScaler 的 CVE 清单。

您可以根据需要通过单击 + 号来添加或删除这些列中的任何一列。



要修复漏洞问题，请选择 NetScaler 实例并应用建议的补救措施。大多数 CVE 需要升级作为补救措施，而其他的 CVE 则需要升级和额外的补救措施。

- 有关 CVE-2020-8300 补救措施，请参阅 修复 CVE-2020-8300 的漏洞。
- 对于 CVE-2021-22927 和 CVE-2021-22920，请参阅 修复 CVE-2021-22927 和 CVE-2021-22920 的漏洞。
- 对于 CVE CVE-2021-22956，请参阅 识别和修复 CVE-2021-22956 的漏洞
- 对于 CVE CVE-2022-27509，请参阅 修复 CVE-2022-27509 的漏洞

> 注意
>
> 如果您的 NetScaler 实例有自定义设置，请在规划 NetScaler 升级之前，请参阅自定义 NetScaler 配置的升级注意事项 。

升级：您可以将易受攻击的 NetScaler 实例升级到具有修复程序的版本和版本。此详细信息可以在修复列中看到。要升级，请选择实例，然后单击 继续升级工作流程。在升级工作流程中，易受攻击的 NetScaler 会自动填充为目标 NetScaler。

> 注意
>
> 12.0、11,0、10.5 及更低版本已经结束了生命周期（EOL）。如果您的 NetScaler 实例正在这些版本中的任何一个版本上运行，请升级到支持的版本。

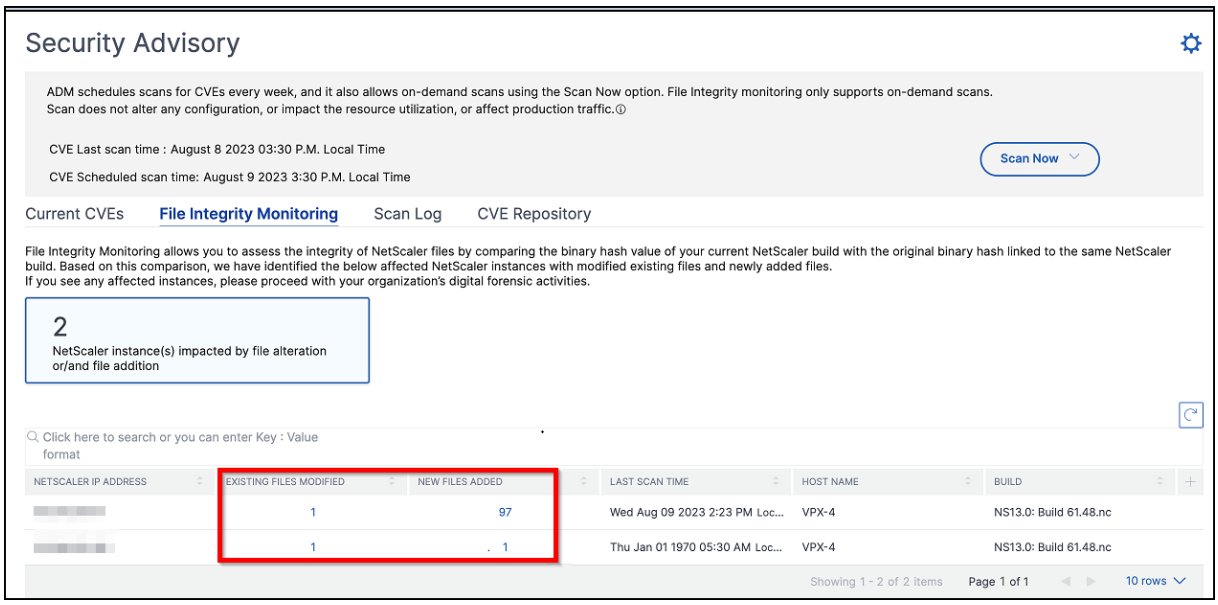
升级工作流程启动。有关如何使用 NetScaler 控制台升级 NetScaler 实例的更多信息，请参见使用作业升级 NetScaler 实例。

> 注意
>
> 要升级到的版本和版本由您自行决定。请参阅“修复”栏下的建议，了解哪些版本和版本已修复安全问题。因此，选择支持的版本和版本，该版本尚未到生命周期结束。

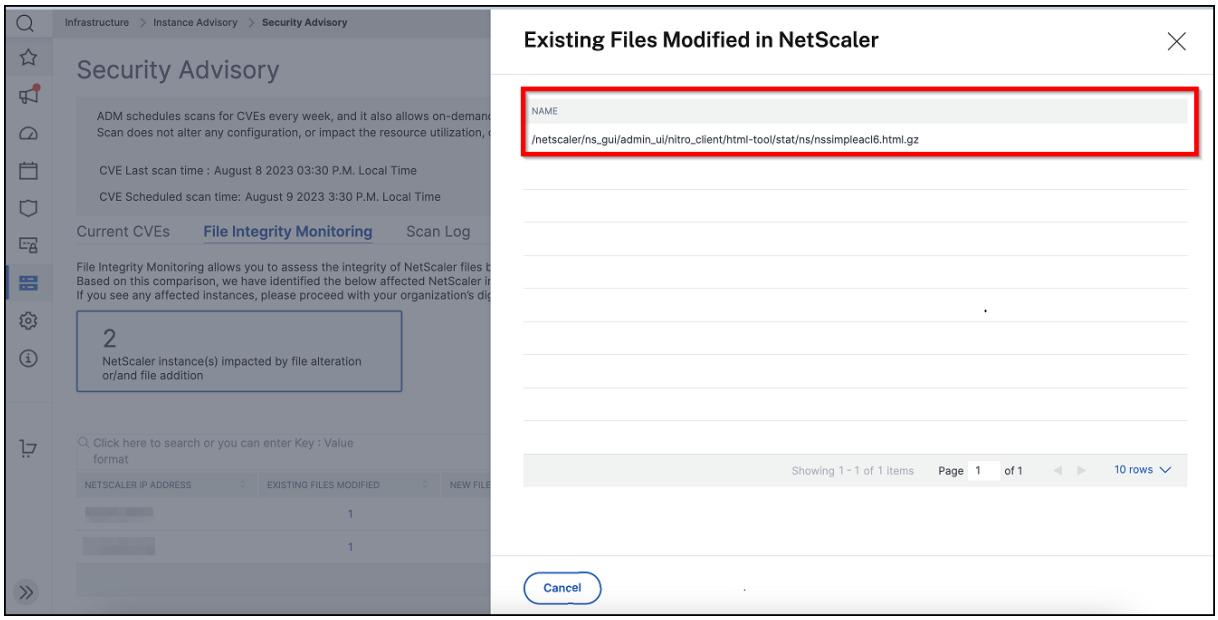
文件完整性监视

此选项卡显示 NetScaler 实例的文件完整性监视扫描结果，这些实例对原始 NetScaler 构建文件进行了任何修改或添加。

以下示例显示了两个受影响的 NetScaler 实例的扫描结果，其中修改了现有文件并将新文件添加到原始构建文件中。

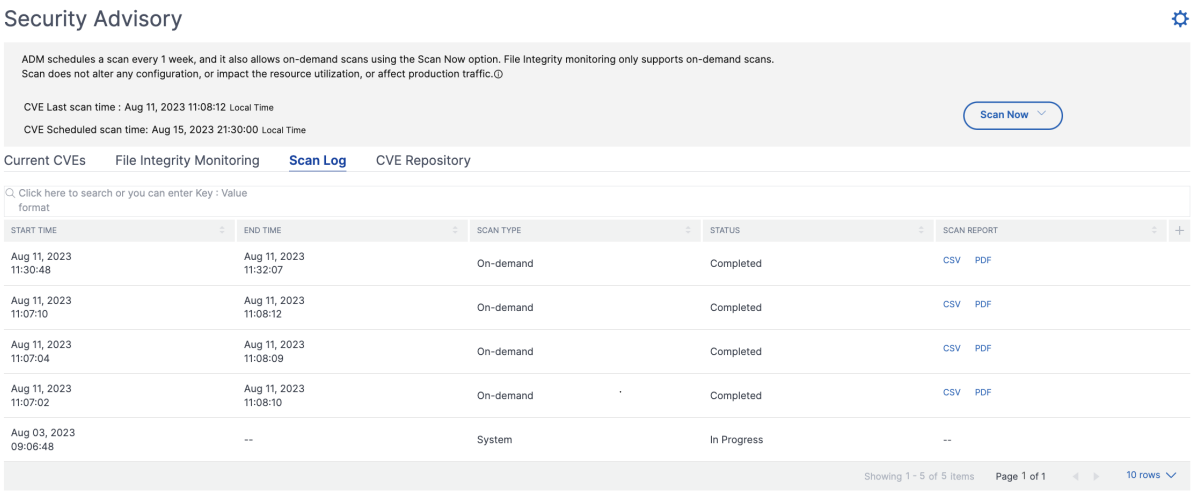


单击“已修改的现有文件”和“已 添加的新文件”下的数字以查看详细信息。



扫描日志（仅适用于 **CVE**）

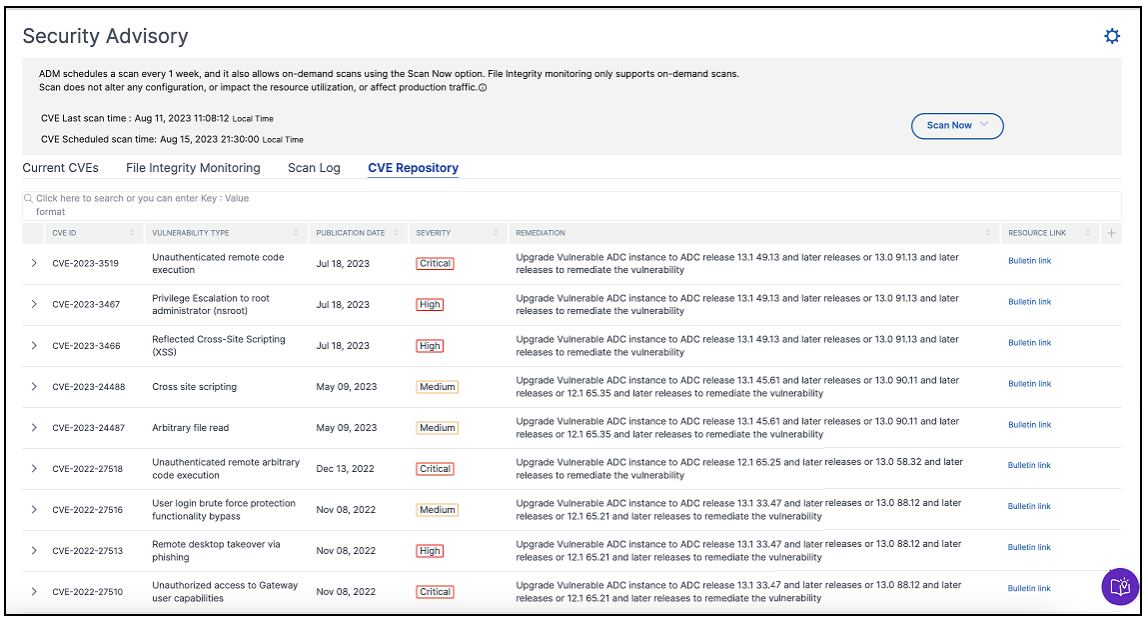
该选项卡显示最近五次 CVE 扫描的报告，其中包括默认系统扫描和用户启动的按需扫描。您可以下载 CSV 格式的每次扫描报告。如果按需扫描正在进行中，您可以在此处看到完成状态。如果任何扫描失败，则状态表示失败。



CVE 存储库

此选项卡包含 2019 年 12 月以来所有 CVE 的最新信息，以及以下详细信息：

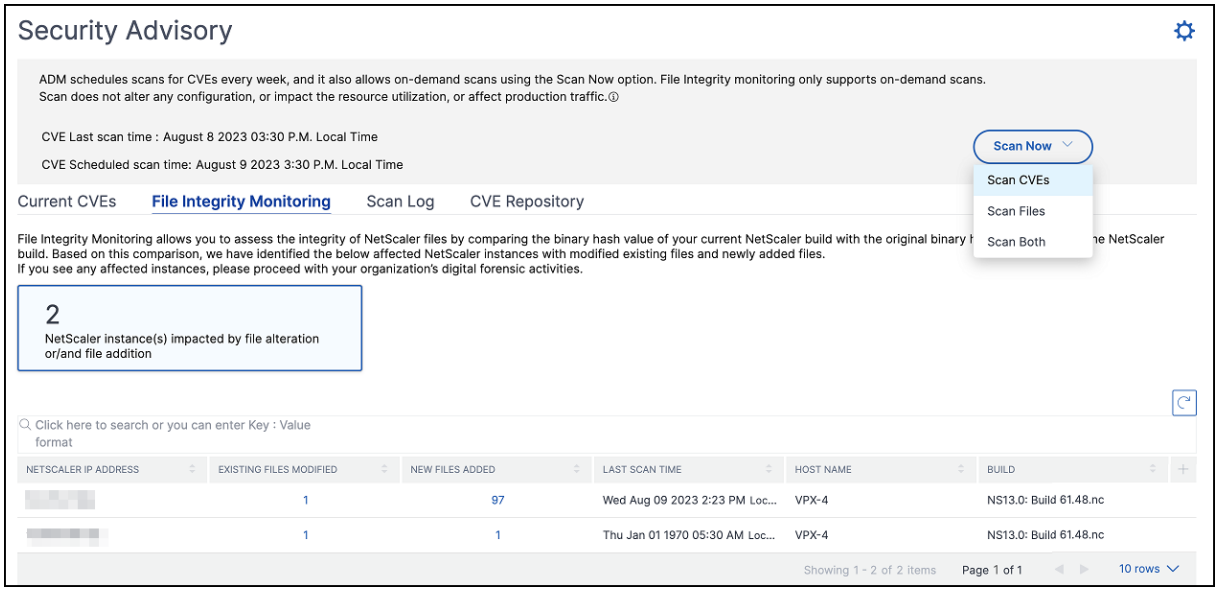
- CVE ID
- 漏洞类型
- 发布日期
- 严重性级别
- 补救措施
- 安全公告链接



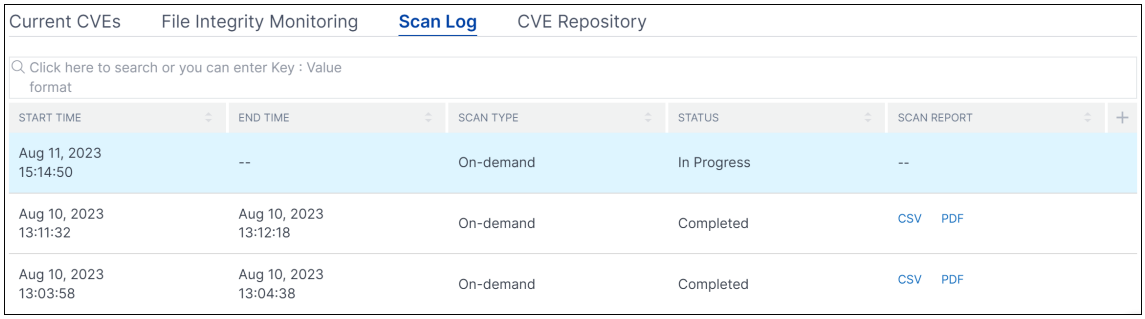
立即扫描

您可以根据需要随时扫描实例。

单击“立即扫描”，然后选择“扫描 **CVE**”、“扫描文件”或“同时扫描”以获取您的实例的最新安全报告。



- 扫描 **CVE** -仅扫描影响您的 NetScaler 实例的 CVE。扫描完成后，修改后的安全详细信息将显示在安全公告 GUI 中。您还可以在“扫描日志”下找到报告，也可以下载该报告。



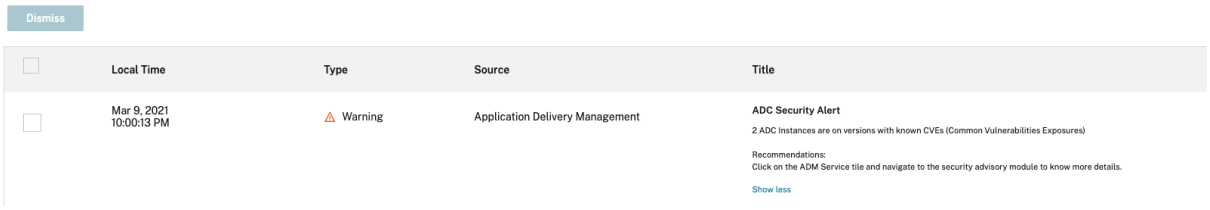
- 扫描文件 -仅扫描文件完整性监视，并在“文件完整性监视”选项卡中提供结果。
- 两者兼而有之 -扫描 CVE 检测和文件完整性监视

NetScaler 控制台需要几分钟才能完成扫描。

> 注意
>
> 扫描日志仅显示最近五次 CVE 扫描的日志，这些扫描既可以是计划的，也可以是按需进行的。

通知（仅适用于 **CVE**）

作为管理员，您会收到 Citrix Cloud 通知，这些通知会告知有多少 NetScaler 实例容易受到 CVE 的攻击。要查看通知，请单击 NetScaler 控制台 GUI 右上角的钟形图标。

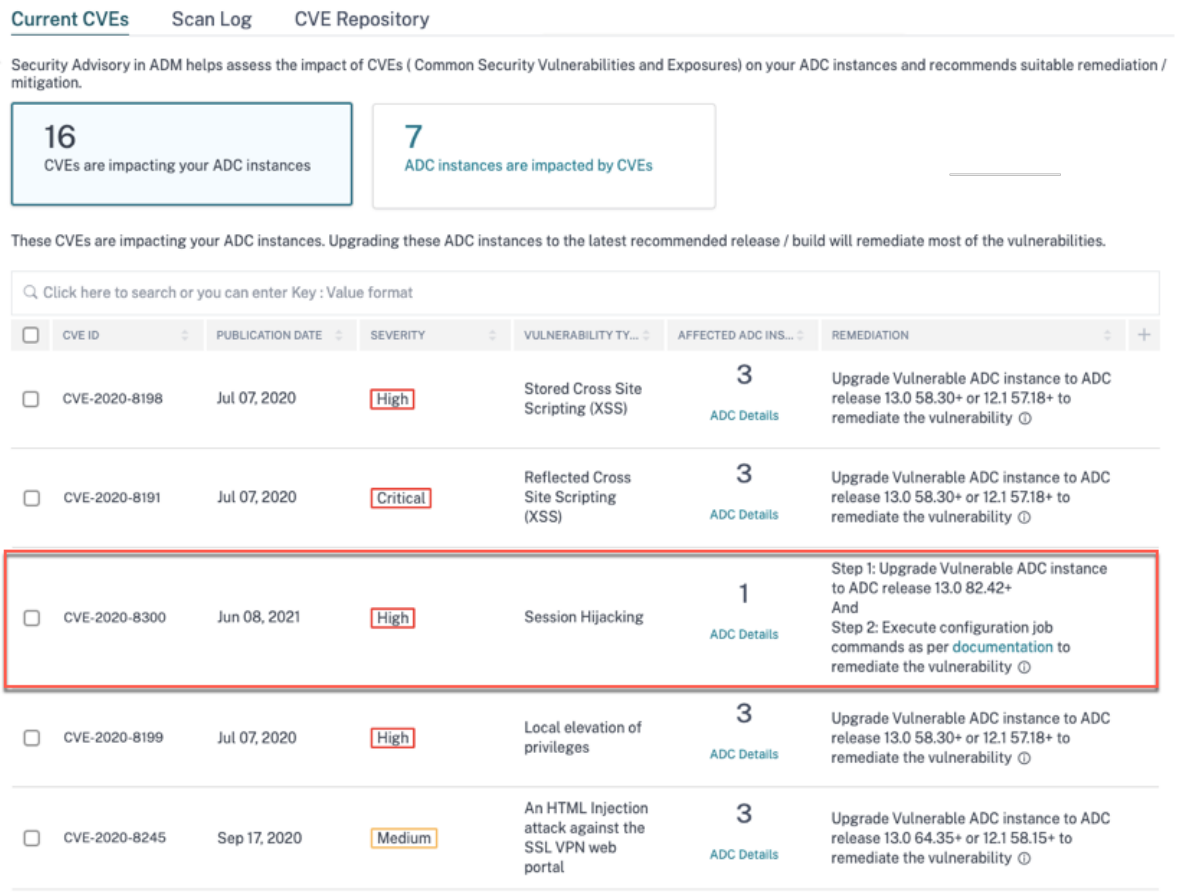


> 免责声明：
>
> 请注意，NetScaler 文件完整性监视（“功能”）无法检测威胁参与者在瞄准相关环境时可能使用的所有技术、策略或程序 (TTP)。威胁参与者经常更改 TTP 和基础设施，因此该功能可能仅限于对某些威胁没有取证价值。强烈建议您保留经验丰富的法医调查人员的服务，以评估您的环境是否存在任何可能的威胁。
>
> 本文档及其包含的信息按原样提供。Cloud Software Group, Inc. 对文档或其内容不作任何明示或暗示的保证或陈述，包括但不限于本文档或其中包含的信息没有错误或符合任何适销性或适用于特定目的的条件。

修复 **CVE-2020-8300** 的漏洞

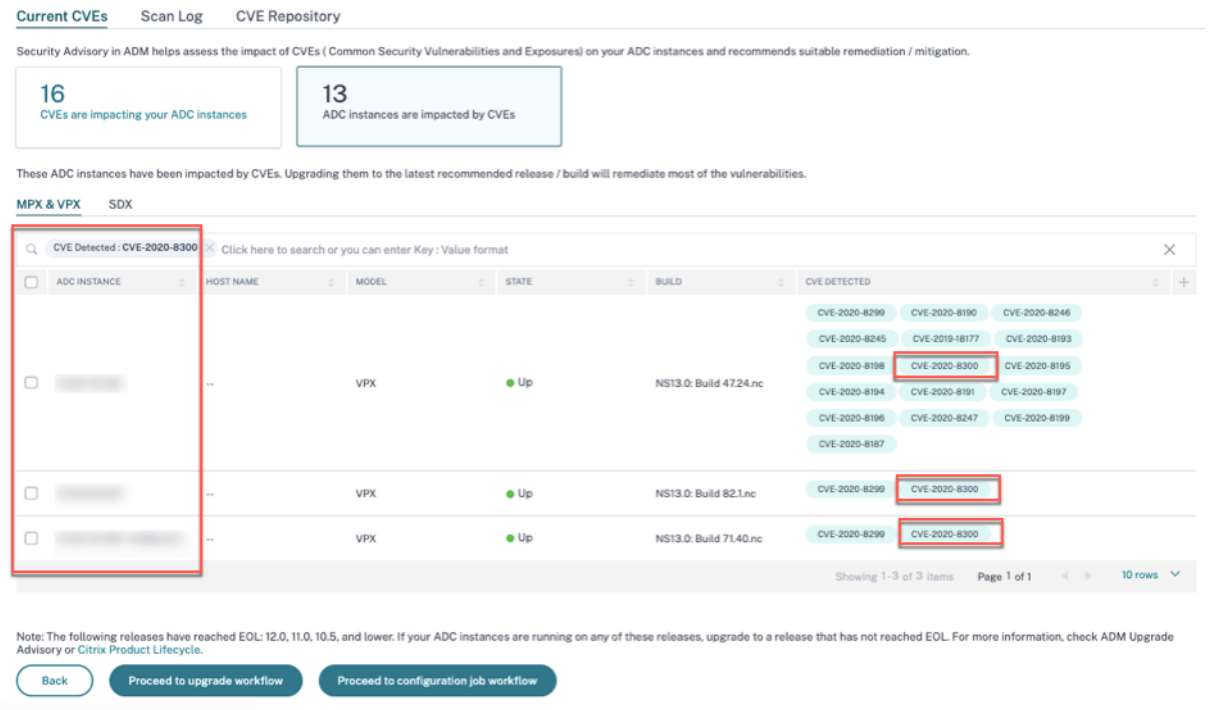
January 29, 2024

在 NetScaler 控制台安全公告控制面板中，在“当前 CVE”**>**“**<number of>NetScaler** 实例受 CVE 影响”下，您可以看到由于该特定 CVE 而易受攻击的所有实例。要查看受 CVE-2020-8300 影响的实例的详细信息，请选择 **CVE-2020-8300** ，然后单击“查看受影响实例”。



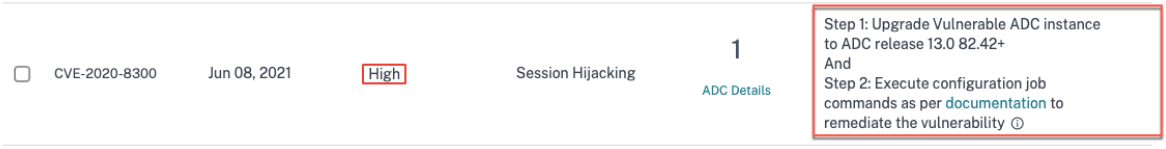
> 注意
>
> 有关安全公告控制板的更多信息，请参阅安全公告。

将出现**<number of>**受 **CVE** 影响的 **NetScaler** 实例窗口。在这里，您可以看到受 CVE-2020-8300 影响的 NetScaler 实例的数量和详细信息。



修复 **CVE-2020-8300**

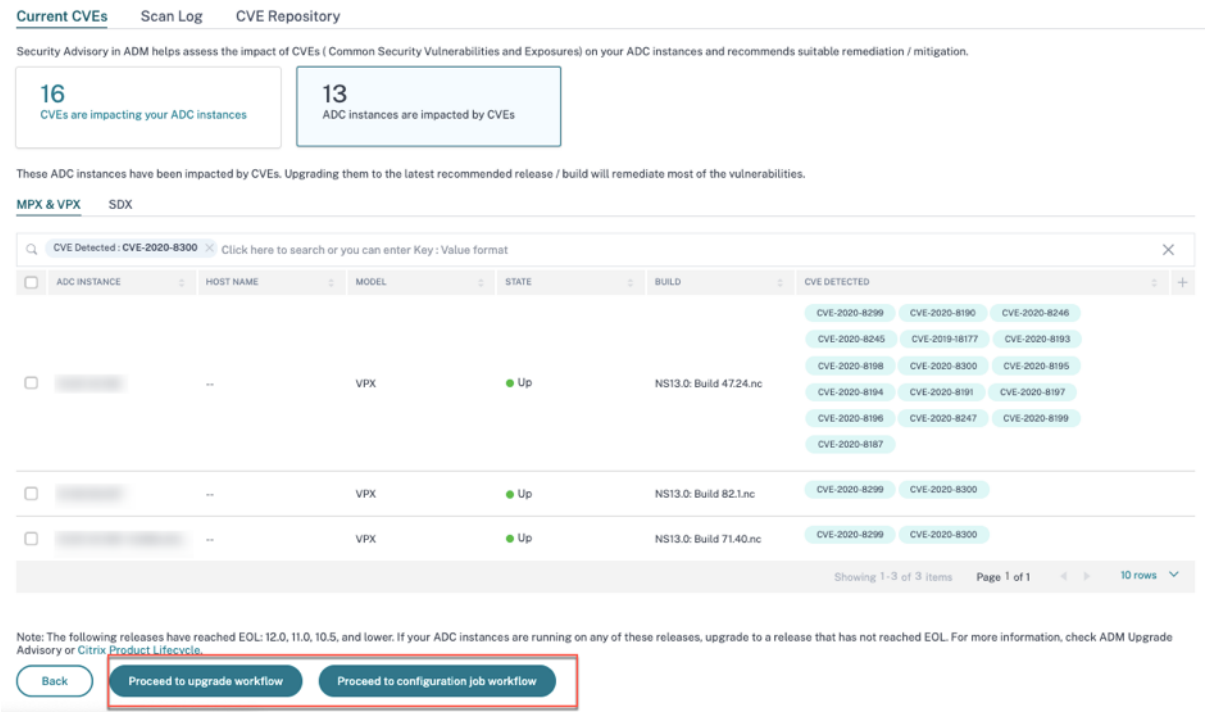
对于受 CVE-2020-8300 影响的 NetScaler 实例，补救过程分为两步。在 GUI 中，在“当前 CVE”**>** “**NetScaler** 实例受 CVE 影响”下，您可以看到第 1 步和第 2 步。



这两个步骤包括：

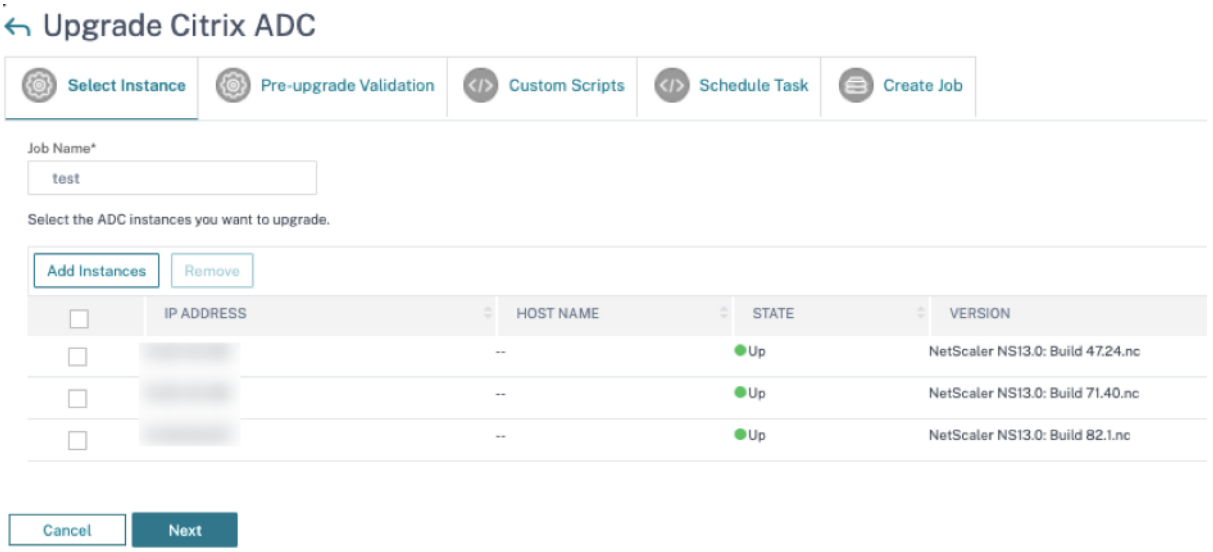
1. 将易受攻击的 NetScaler 实例升级到具有修复程序的版本和版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。对每个易受攻击的 NetScaler 执行此步骤，一次只能执行一个操作，并包括该 NetScaler 的所有 SAML 操作和 SAML 配置文件。

在“当前 **CVE>** 受 **CVE** 影响的 **NetScaler** 实例”下，您可以看到此两步修复过程的两个独立工作流程：继续 升级工作流程和继续 配置作业工作流程。



第 **1** 步：升级易受攻击的 **NetScaler** 实例

要升级有漏洞的实例，请选择实例，然后单击“继续”升级工作流程。升级流程在已填充易受攻击的 NetScaler 实例的情况下打开。



有关如何使用 NetScaler 控制台升级 NetScaler 实例的详细信息，请参见创建 NetScaler 升级任务。

> 注意
>
> 对于所有易受攻击的 NetScaler 实例，可以立即执行此步骤。

步骤 **2**：应用配置命令

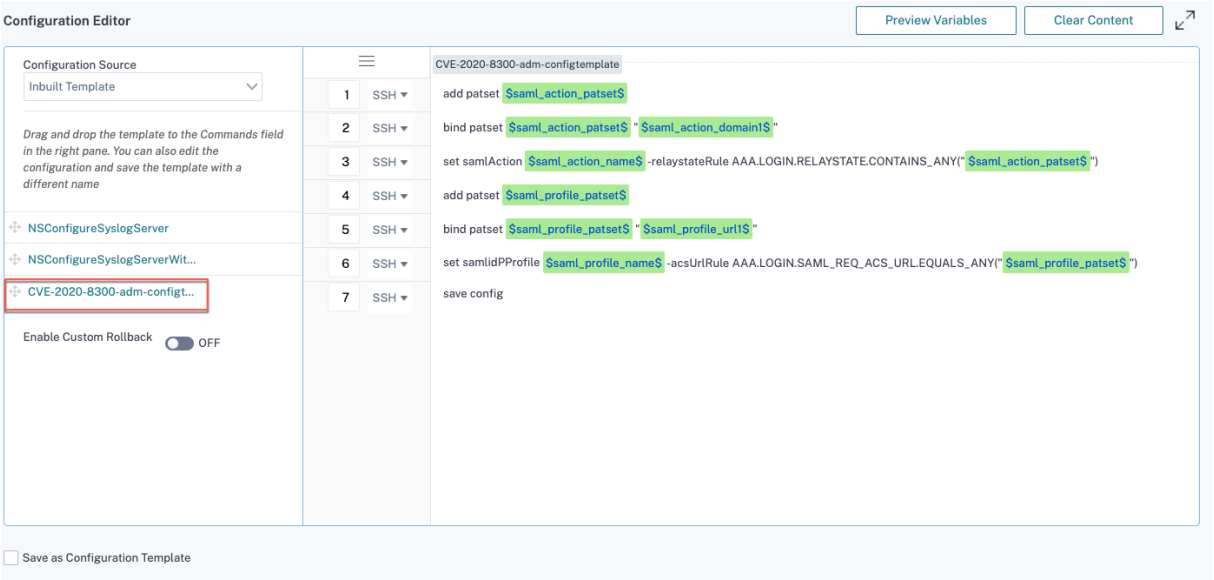
升级受影响的实例后，在 **<number of>** 受 **CVE** 影响的 **NetScaler** 实例窗口中，选择一个受 CVE-2020-8300 影响的实例，然后 点击继续配置作业流程。该工作流程包括以下步骤。

1. 自定义配置。
2. 查看自动填充的受影响实例。
3. 为作业的变量指定输入。
4. 查看填充变量输入的最终配置。
5. 运行作业。

在选择实例并单击“继续配置作业工作流程”之前，请记住以下几点：

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择该实例并 单击“继续进行配置作业工作流程”时，内置配置模板不会自动填充在“选择配置”下。手动将安全公告模板下的相应配置作业模板拖放到右侧的配置作业窗格中。
- 对于仅受 CVE-2021-22956 影响的多个 NetScaler 实例：您可以同时在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，它们都只受到 CVE-2021-22956 的影响。选择所有这些实例，然后单击“继续配置作业工作流程”，内置配置模板将自动填充在“选择配置”下。请参阅 发行说明中的已知问题 NSADM-80913。
- 对于受 CVE-2021-22956 影响的多个 NetScaler 实例以及一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920），这些实例需要同时对每个 NetScaler 进行补救：当您选择这些实例并 单击“继续配置作业流程”时，会出现一条错误消息，提示您一次在每个 NetScaler 上运行配置作业。

步骤 **1**：选择配置　在配置作业工作流中，内置配置模板会自动填充在“选择配置”下。



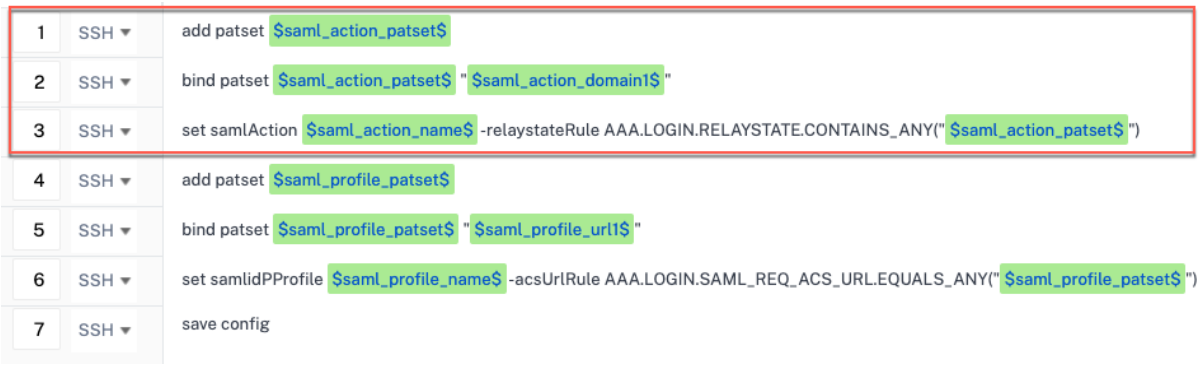
为每个受影响的 NetScaler 实例运行一个单独的配置作业，并包括该 NetScaler 的所有 SAML 操作和 SAML 配置文件。例如，如果您有两个易受攻击的 NetScaler 实例，每个实例都有两个 SAML 操作和两个 SAML 配置文件，则必须运行此配置作业两次。每个 NetScaler 一次，涵盖其所有 SAML 操作和 SAML 配置文件。

NetScaler 1	NetScaler 2
任务 1：两个 SAML 操作 + 两个 SAML 配置文件	任务 2：两个 SAML 操作 + 两个 SAML 配置文件

为作业命名并根据以下规范自定义模板。内置配置模板只是大纲或基础模板。根据您的部署自定义模板以满足以下要求：

a.**SAML** 操作及其关联域

根据您在部署中执行的 SAML 操作的数量，您必须复制第 1—3 行并为每个 SAML 操作自定义域。



例如，如果您有两个 SAML 操作，则重复第 1—3 行两次，然后相应地为每个 SAML 操作自定义变量定义。

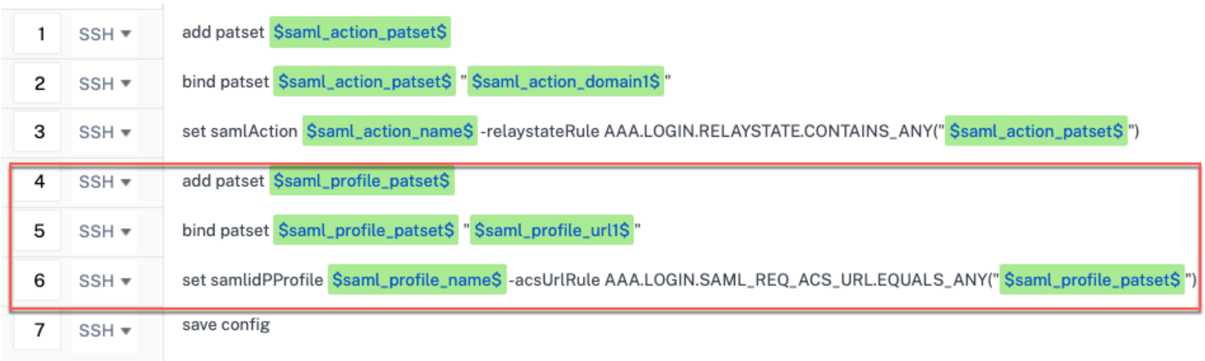
而且，如果您有一个 SAML 操作有 N 个域，则必须手动多次键入行 `bind patset $saml_action_patset$ “$saml_action_domain1$”` ，以确保该行在该 SAML 操作中出现 N 次。并更改以下变量定义名称：

- `saml_action_patset`：是配置模板变量，它表示 SAML 操作的模式集（patset）名称的值。您可以在配置作业工作流程的第 3 步中指定实际值。请参阅本文档中的步骤 3：指定变量值部分。
- `saml_action_domain1`：是配置模板变量，它代表该特定 SAML 操作的域名。您可以在配置作业工作流程的步骤 3 中指定实际值。请参阅本文档中的步骤 3：指定变量值部分。

要查找设备的所有 SAML 操作，请运行命令 `show samlaction`。

b. **SAML** 配置文件及其关联的 **URL**

根据您在部署中拥有的 SAML 配置文件数量，复制行 4—6。自定义每个 SAML 配置文件的 URL。



例如，如果您有两个 SAML 配置文件，请手动输入两行 4—6 行，然后相应地为每个 SAML 操作自定义变量定义。

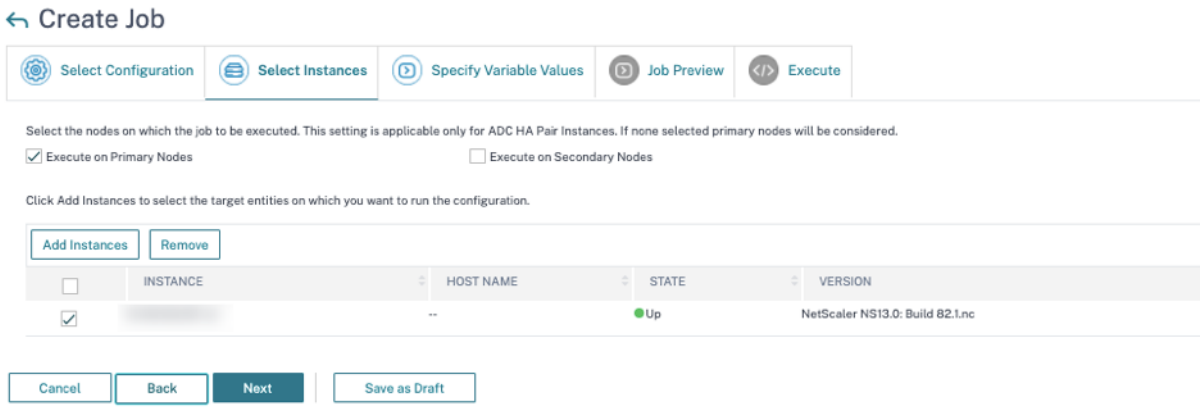
而且，如果您有一个 SAML 操作有 N 个域，则必须手动 `bind patset $saml_profile_patset$ “$saml_profile_url1$”` 多次键入该行，以确保该行在该 SAML 配置文件中出现 N 次。并更改以下变量定义名称：

- `saml_profile_patset`：是配置模板变量，它表示 SAML 配置文件的模式集（patset）名称的值。您可以在配置作业工作流程的步骤 3 中指定实际值。请参阅本文档中的步骤 3：指定变量值部分。
- `saml_profile_url1`：是配置模板变量，它代表该特定 SAML 配置文件的域名。您可以在配置作业工作流程的步骤 3 中指定实际值。请参阅本文档中的步骤 3：指定变量值部分。

要查找设备的所有 SAM 配置文件，请运行命令 `show samlidpProfile`。

步骤 **2**：选择实例

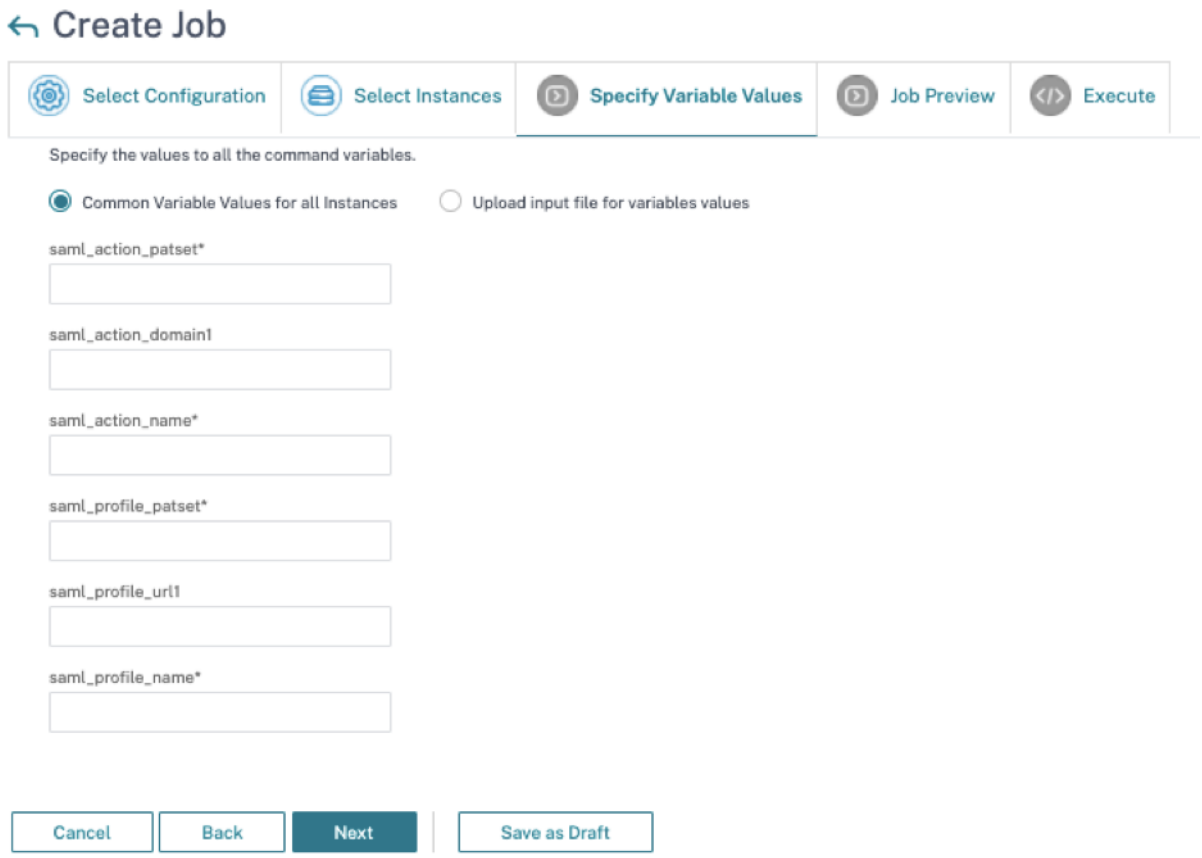
受影响的实例会在“选择实例”下自动填充。选择实例，然后单击“下一步”。



步骤 **3**：指定变量值　输入变量值。

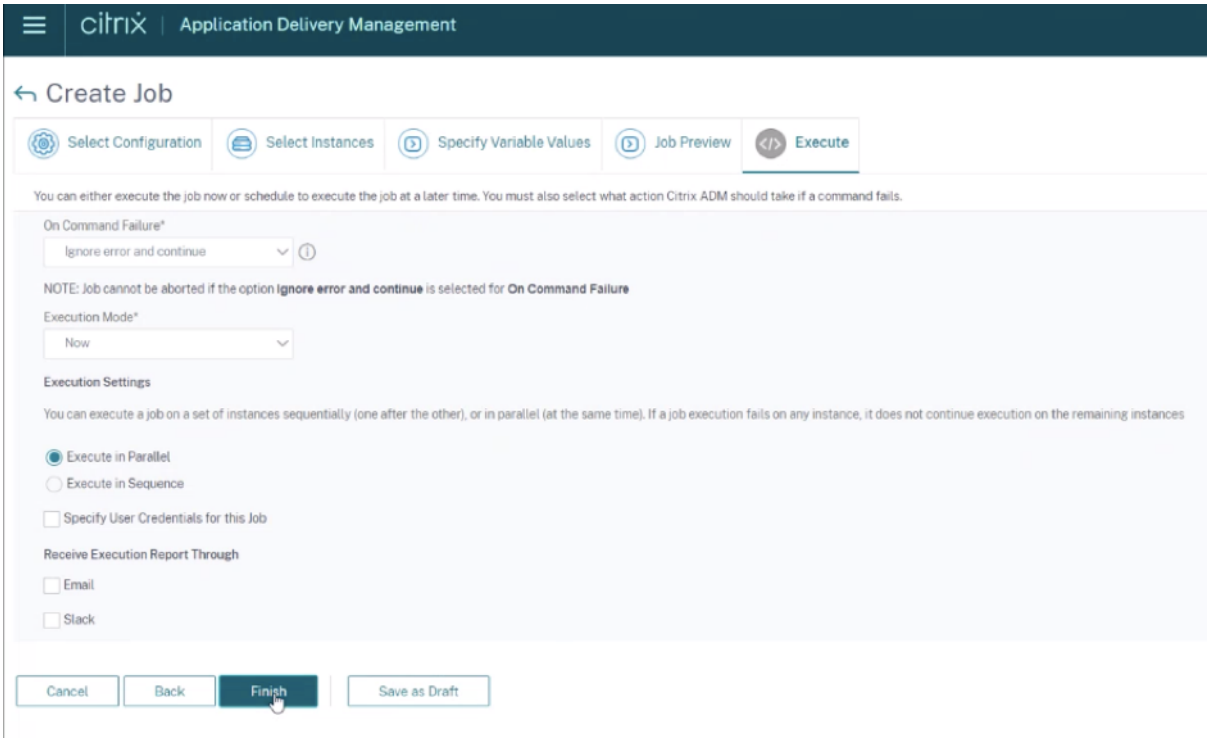
- `saml_action_patset`：为 SAML 操作添加一个名称
- `saml_action_domain1`：按 `https://<example1.com>/` 格式输入域名
- `saml_action_name`：输入与您为其配置作业的 SAML 操作相同的内容
- `saml_profile_patset`: 为 SAML 配置文件添加一个名称
- `saml_profile_url1`：输入 URL 采用这种格式 `https://<example2.com>/cgi/samlauth`
- `saml_profile_name`：输入与您为其配置作业的 SAML 配置文件相同的配置文件

> 注意
>
> 对于 URL，扩展名并不总是如此 `cgi/samlauth`。这取决于您拥有的第三方授权，因此您必须输入扩展名。



步骤 **4**：预览配置　预览配置中已插入的变量值，然后单击“下一步”。

步骤 **5**：运行作业　单击“完成”运行配置作业。



作业运行后，它会显示在 基础结构 **>** 配置 **>** 配置作业下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修改后的安全状况。

NetScaler 控制台 **Express** 帐户的注意事项

NetScaler 控制台 Express 帐户的功能有限，其中包括仅限两个配置任务。要了解有关 NetScaler 控制台 Express 帐户的更多信息，请参见 使用 Express 帐户管理 NetScaler Console 资源。
对于 CVE-2020-8300 补救，必须运行与易受攻击的 NetScaler 实例数量一样多的配置作业。因此，如果您有 Express 帐户并且需要运行两个以上的配置作业，请遵循此解决方法。

解决办法：为两个易受攻击的 NetScaler 实例运行两个配置作业，然后删除这两个作业，继续为接下来的两个易受攻击的 NetScaler 实例运行接下来的两个作业。继续执行此操作，直到覆盖完所有易受攻击的实例。在删除作业之前，您可以下载报告以备将来参考。要下载报告，请在“网络”**>**“作业”下选择作业，然后单击“操作”下的“下载”。

示例：如果您有六个易受攻击的 NetScaler 实例，请分别在两个易受攻击的实例上运行两个配置作业，然后删除这两个配置作业。再重复此步骤两次。最后，您将分别为六个 NetScaler 实例运行六个配置作业。在 NetScaler 控制台用户界面的“基础架构”**>**“任务”下，您只能看到最后两个配置作业。

场景

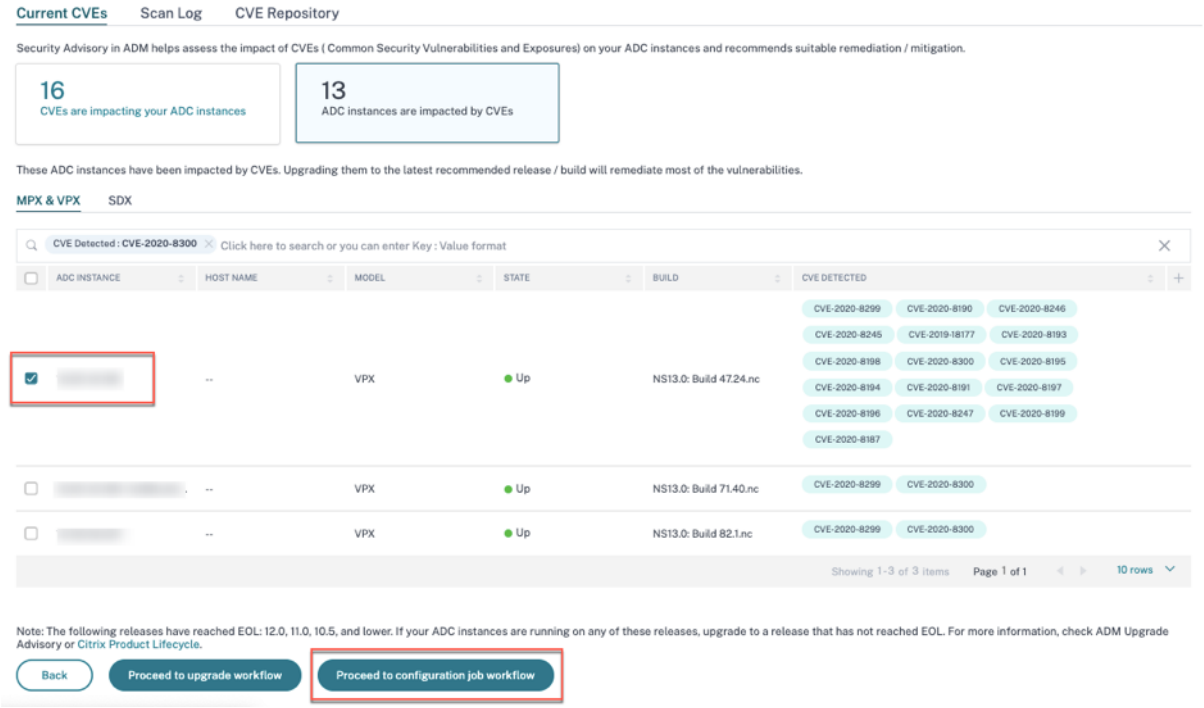
在这种情况下，三个 NetScaler 实例易受 CVE-2020-8300 攻击，您需要修复所有实例。请按照以下步骤进行操作：

1. 按照本文档的“升级实例”部分中给出的步骤，升级所有三个 NetScaler 实例。

2. 使用配置作业流程，一次将配置补丁应用到一个 NetScaler 上。请参阅本文档“应用配置命令”部分中给出的步骤。

易受攻击的 NetScaler 1 具有以下配置：

两个 SAML 操作	两个 SAML 配置文件
SAML 操作 1 有一个域，而 SAML 操作 2 有两个域	SAML 配置文件 1 有一个 URL，而 SAML 配置文件 2 有两个 URL



选择 NetScaler 1，然后 单击“继续配置作业流程”。内置模板会自动填充。接下来，给出作业名称并根据给定的配置自定义模板。

下表列出了自定义参数的变量定义。

表 1. SAML 操作的变量定义

NetScaler 配置	patset 的变量定义	SAML 操作名称的变量定义	域的变量定义
SAML 操作 1 有一个域	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML 操作 2 有两个域	saml_action_patset2	saml_action_name2	saml_action_domain2、saml_action_domain3

表 2. SAML 配置文件的变量定义

NetScaler 配置	patset 的变量定义	SAML 配置文件名称的变量定义	URL 的变量定义
SAML 配置文件 1 有一个 URL	saml_profile_patset1	saml_profile_name1	saml_profile_url1
SAML 配置文件 2 有两个 URL	saml_profile_patset2	saml_profile_name2	saml_profile_url2、saml_profile_url3

在“选择实例”下，选择 NetScaler 1，然后单击“下一步”。将出现“指定变量值”窗口。在此步骤中，您需要为上一步中定义的所有变量提供值。

接下来，查看变量。

单击“下一步”，然后单击“完成”以运行作业。

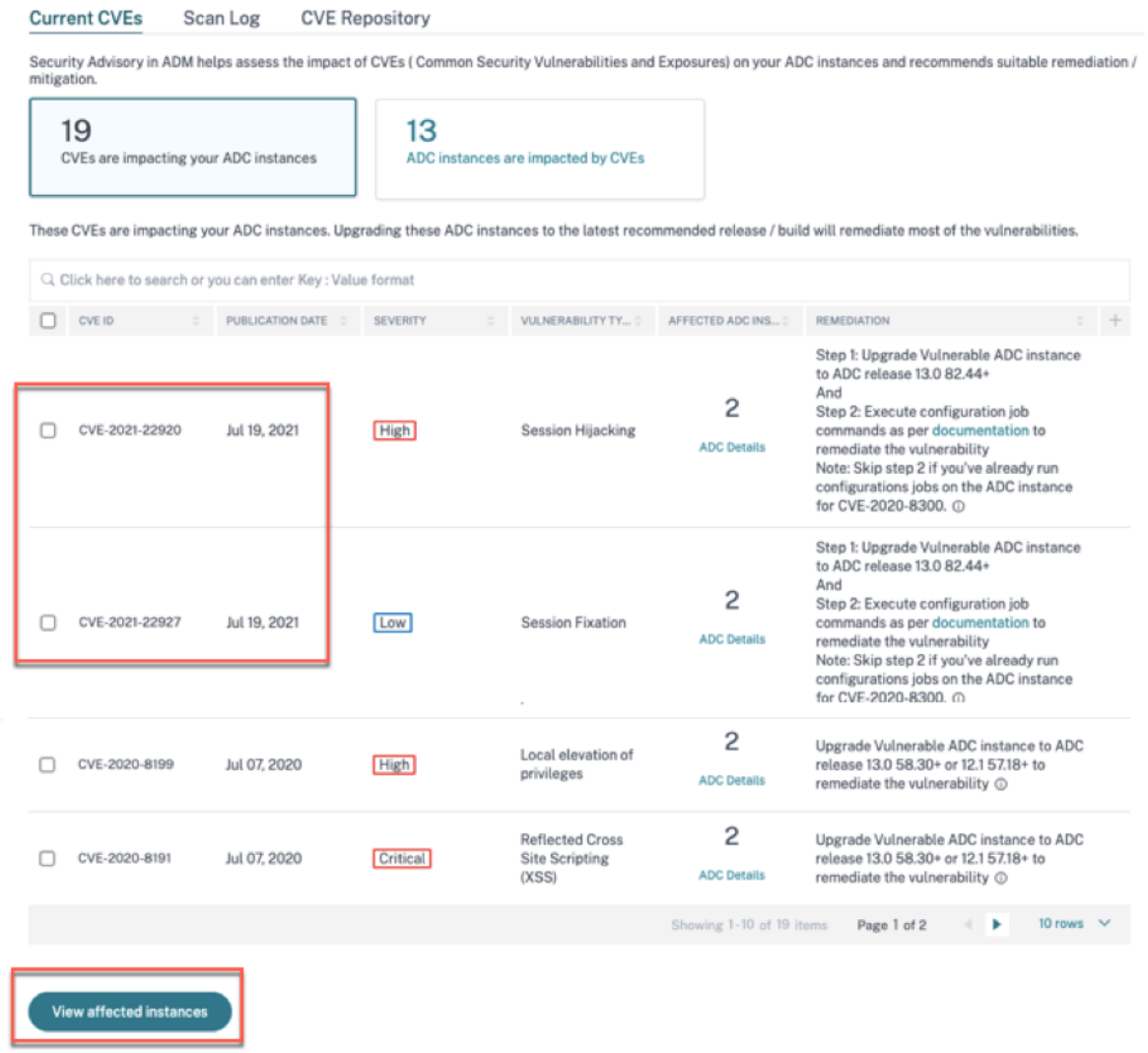
作业运行后，它会显示在 基础结构 **>** 配置 **>** 配置作业下。

完成 NetScaler 1 的两个修复步骤后，按照相同的步骤修复 NetScaler 2 和 NetScaler 3。修复完成后，您可以运行按需扫描以查看修改后的安全状态。

修复 **CVE-2021-22927** 和 **CVE-2021-22920** 的漏洞

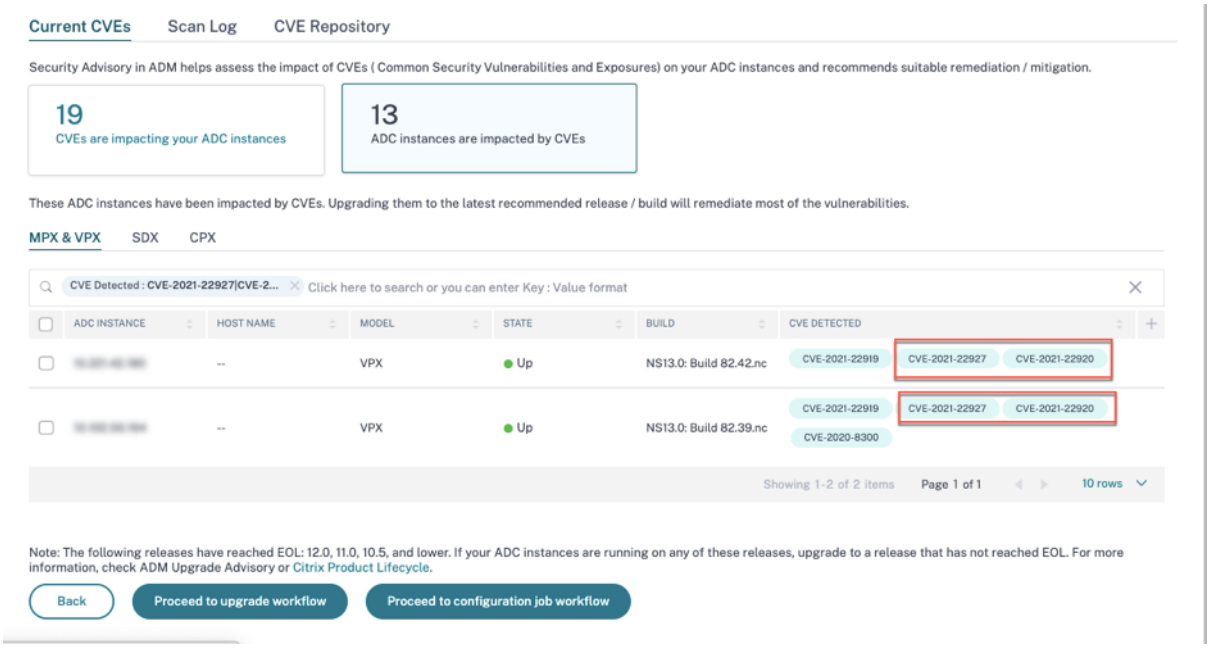
January 29, 2024

在 NetScaler 控制台安全公告控制面板中，在“当前 CVE” **>** “**<number of>NetScaler** 实例受 CVE 影响”下，您可以看到所有因 CVE-2021-22927 和 CVE-2021-22920 而易受攻击的实例。要查看受这两个 CVE 影响的实例的详细信息，请选择一个或多个 CVE，然后单击“查看受影响的实例”。



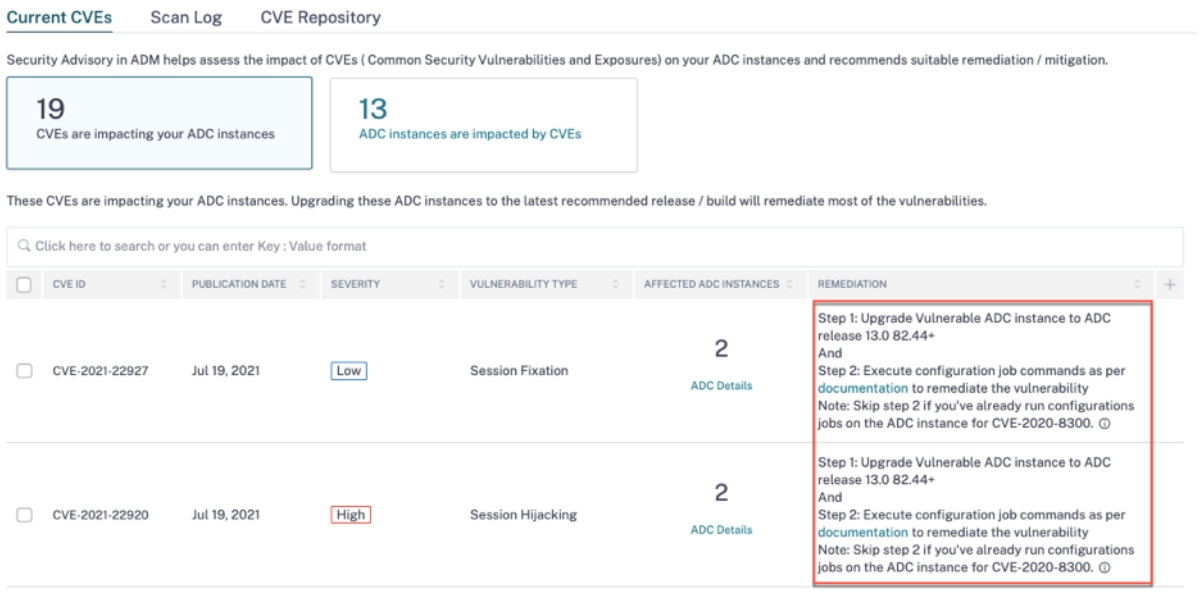
> 注意
>
> 安全公告系统扫描可能需要几个小时才能得出结论，并在安全建议模块中反映 CVE-2021-22927 和 CVE-2021-22920 的影响。要更快地查看影响，请单击“立即扫描”开始按需扫描。
>
> 有关安全公告控制面板的更多信息，请参阅安全公告。

将出现**<number of>**受 **CVE** 影响的 **NetScaler** 实例窗口。在以下屏幕截图中，您可以看到受 CVE-2021-22927 和 CVE-2021-22920 影响的 NetScaler 实例的数量和详细信息。



修复 **CVE-2021-22927** 和 **CVE-2021-22920**

对于受 CVE-2021-22927 和 CVE-2021-22920 影响的 NetScaler 实例，修复过程分为两步。在 GUI 中，在“当前 CVE”**>**“**NetScaler** 实例受 CVE 影响”下，您可以看到第 1 步和第 2 步。

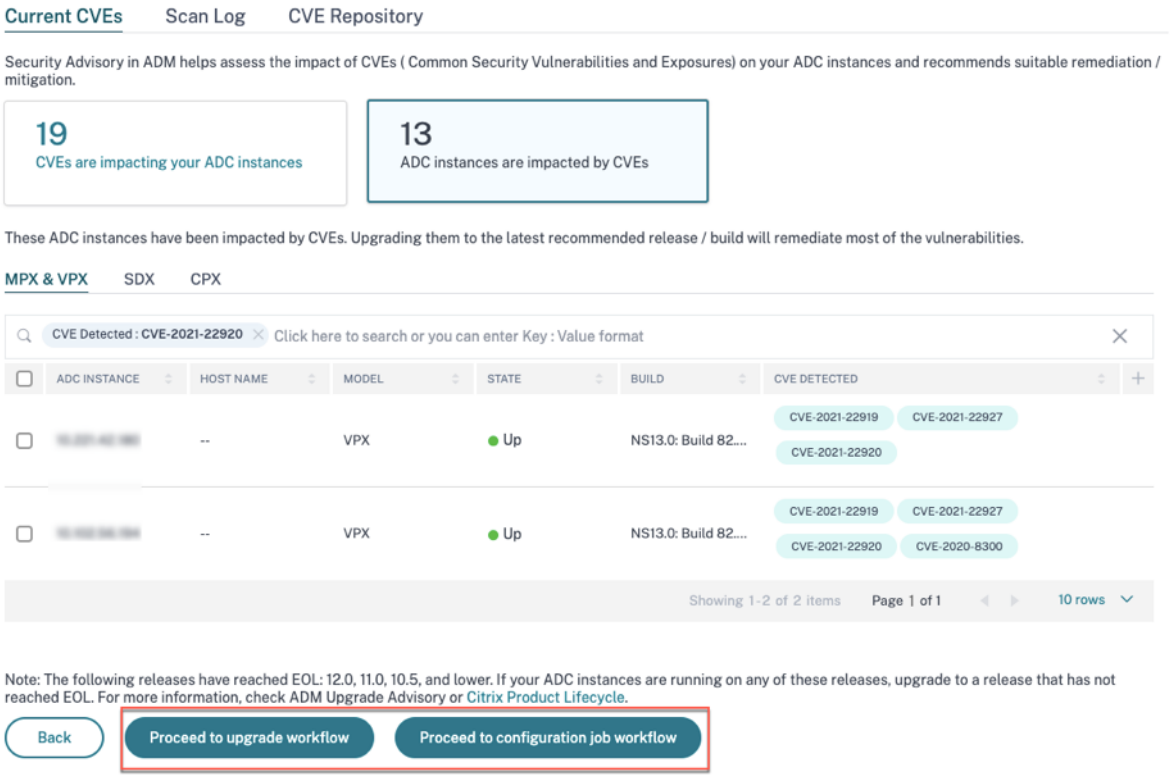


这两个步骤包括：

1. 将易受攻击的 NetScaler 实例升级到具有修复程序的版本和版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。对每个易受攻击的 NetScaler 执行此步骤，一次执行一个，并包括针对该 NetScaler 的所有 SAML 操作。

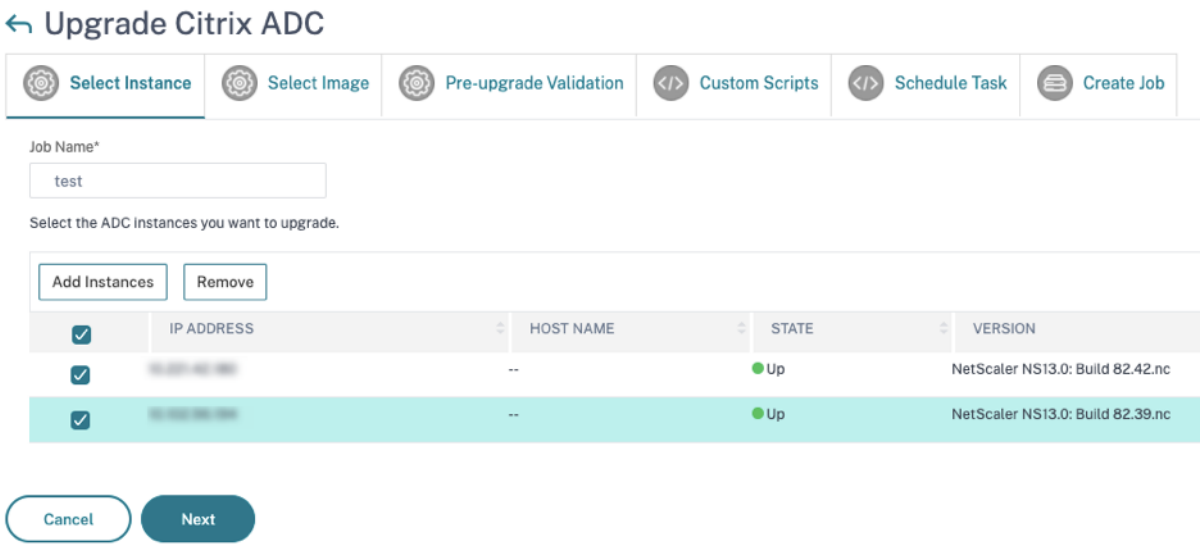
> 注意
>
> 如果您已经在 CVE-2020-8300 的 NetScaler 实例上运行了配置作业，请跳过步骤 2。

在“当前 **CVE>** 受 **CVE** 影响的 **NetScaler** 实例”下，您可以看到此两步修复过程的两个独立工作流程：继续 升级工作流程和继续 配置作业工作流程。



第 **1** 步：升级易受攻击的 **NetScaler** 实例

要升级有漏洞的实例，请选择实例，然后单击“继续”升级工作流程。升级流程在已填充易受攻击的 NetScaler 实例的情况下打开。



有关如何使用 NetScaler 控制台升级 NetScaler 实例的详细信息，请参见创建 NetScaler 升级任务。

> 注意
>
> 对于所有易受攻击的 NetScaler 实例，可以立即执行此步骤。
>
> 注意
>
> 完成所有易受 CVE-2021-22920 和 CVE-2021-22927 攻击的 NetScaler 实例的步骤 1 后，进行按需扫描。当前 CVE 下更新的安全态势可帮助您了解 NetScaler 实例是否仍然容易受到任何 CVE 的攻击。从新状态来看，您还可以检查是否需要运行配置作业。
>
> 如果您已经对适用于 CVE-2020-8300 的 NetScaler 实例应用了相应的配置作业，并且现在您已经升级了 NetScaler 实例，则在进行按需扫描后，该实例将不再显示为 CVE-2020-8300、CVE-2021-22920 和 CVE-2021-22927 易受攻击。

步骤 **2**：应用配置命令

升级受影响的实例后，在 **<number of>** 受 **CVE** 影响的 **NetScaler** 实例窗口中，选择一个受 CVE-2021-22927 和 CVE-2021-22920 影响的实例，然后 点击继续配置作业流程。该工作流程包括以下步骤。

1. 自定义配置。
2. 查看自动填充的受影响实例。
3. 为作业的变量指定输入。
4. 查看填充变量输入的最终配置。
5. 运行作业。

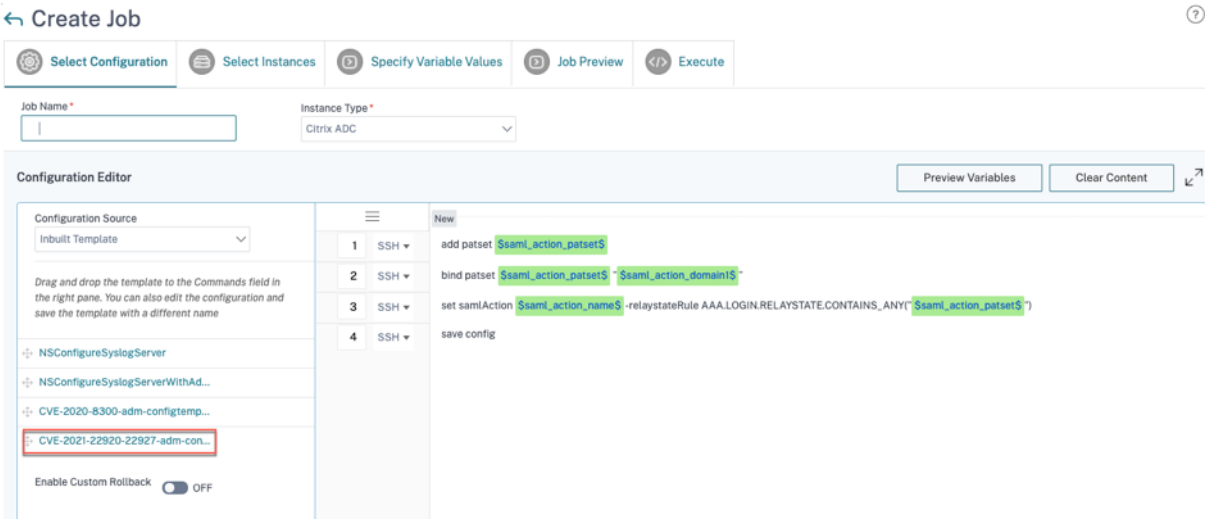
在选择实例并单击“继续配置作业工作流程”之前，请记住以下几点：

- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择该实例并 单击“继续进行配置作业工作流程”时，内置配置模板不会自动填充

在“选择配置”下。手动将安全公告模板下的相应配置作业模板拖放到右侧的配置作业窗格中。

- 对于仅受 CVE-2021-22956 影响的多个 NetScaler 实例：您可以同时在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，它们都只受到 CVE-2021-22956 的影响。选择所有这些实例，然后单击“继续配置作业工作流程”，内置配置模板将自动填充在“选择配置”下。请参阅 发行说明中的已知问题 NSADM-80913。
- 对于受 CVE-2021-22956 影响的多个 NetScaler 实例以及一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920），这些实例需要同时对每个 NetScaler 进行补救：当您选择这些实例并 单击“继续配置作业流程”时，会出现一条错误消息，提示您一次在每个 NetScaler 上运行配置作业。

步骤 **1**：选择配置　在配置作业工作流中，内置配置基础模板会自动填充在“选择配置”下。



> 注意
>
> 如果在步骤 2 中选择的用于应用配置命令的 NetScaler 实例易受 CVE-2021-22927、CVE-2021-22920 以及 CVE-2020-8300 的攻击，则系统会自动填充 CVE-2020-8300 的基本模板。CVE-2020-8300 模板是所有三个 CVE 所需的超级配置命令集。根据您的 NetScaler 实例部署和要求自定义此基本模板。

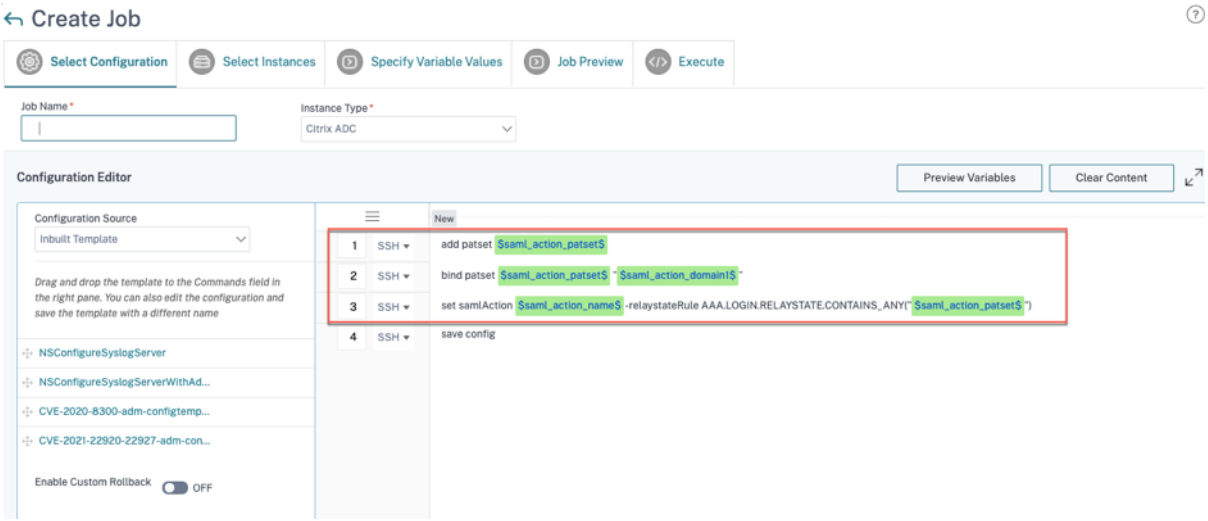
您必须为每个受影响的 NetScaler 实例运行单独的配置作业，一次只能运行一个配置作业，并包括该 NetScaler 的所有 SAML 操作。例如，如果您有两个易受攻击的 NetScaler 实例，每个实例都有两个 SAML 操作，则必须运行此配置作业两次。每个 NetScaler 一次涵盖其所有 SAML 操作。

NetScaler 1	NetScaler2
任务 1：两个 SAML 操作	任务 2：两个 SAML 操作

为作业命名并根据以下规范自定义模板。内置配置模板只是大纲或基础模板。根据您的部署自定义模板以满足以下要求：

a.**SAML** 操作及其关联域

根据您在部署中执行的 SAML 操作的数量，您必须复制第 1—3 行并为每个 SAML 操作自定义域。

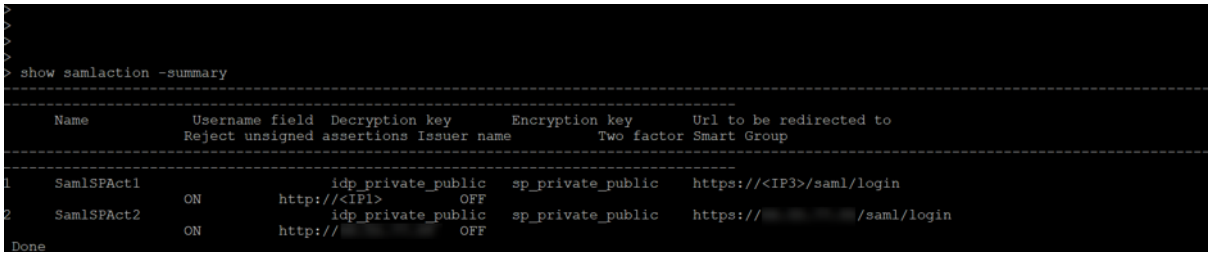


例如，如果您有两个 SAML 操作，则重复第 1—3 行两次，然后相应地为每个 SAML 操作自定义变量定义。

而且，如果您有一个 SAML 操作有 N 个域，则必须手动多次键入行 `bind patset $saml_action_patset$ “$saml_action_domain1$”` ，以确保该行在该 SAML 操作中出现 N 次。并更改以下变量定义名称：

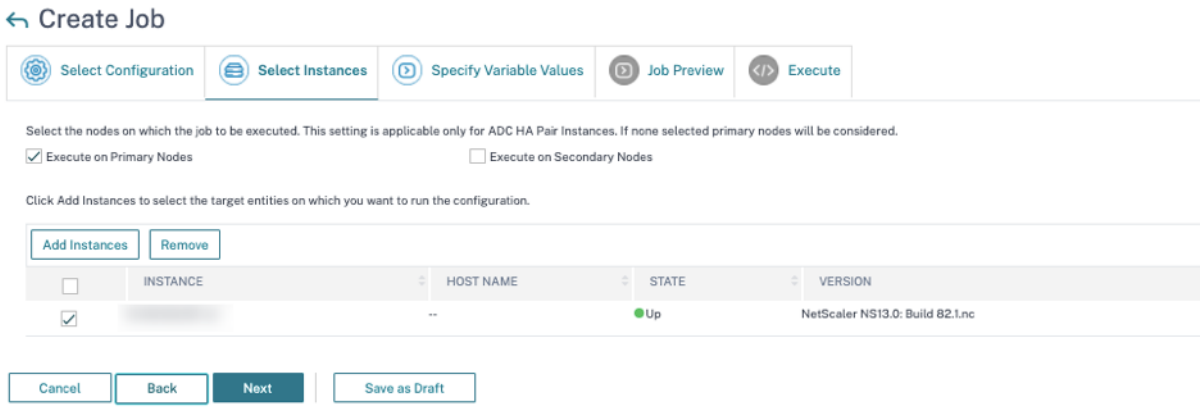
- `saml_action_patset`：是配置模板变量，它表示 SAML 操作的模式集（patset）名称的值。您可以在配置作业工作流程的第 3 步中指定实际值。请参阅本文档中的步骤 3：指定变量值部分。
- `saml_action_domain1`：是配置模板变量，它代表该特定 SAML 操作的域名。您可以在配置作业工作流程的步骤 3 中指定实际值。请参阅本文档中的步骤 3：指定变量值部分。

要查找设备的所有 SAML 操作，请运行命令 `show samlaction`。



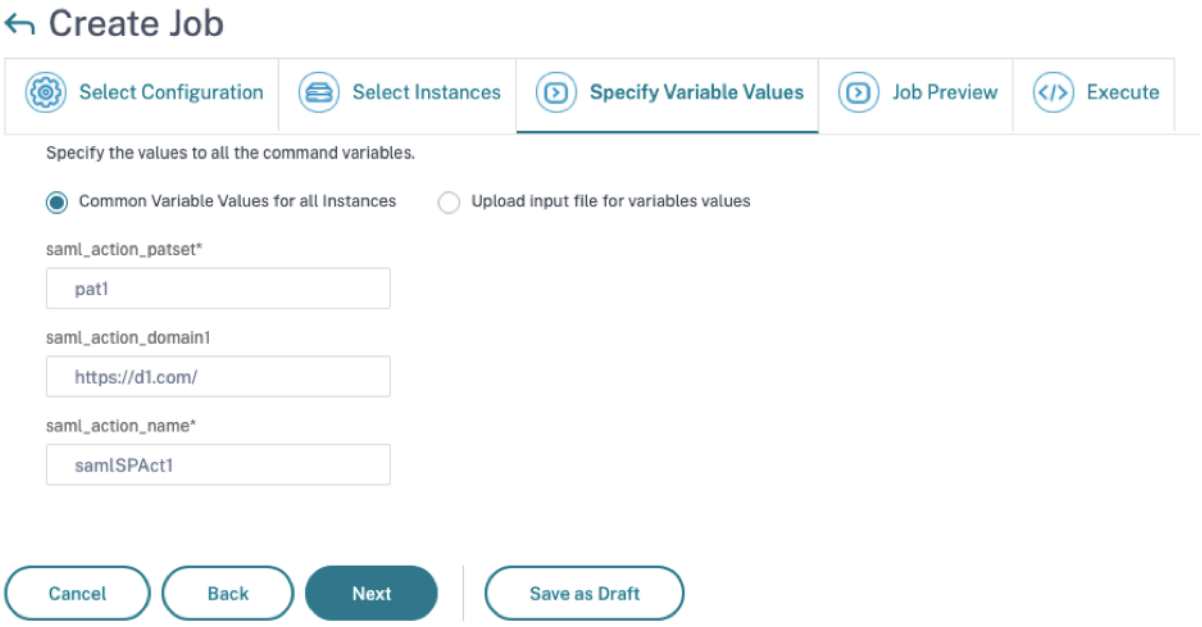
步骤 **2**：选择实例

受影响的实例会在“选择实例”下自动填充。选择实例，然后单击“下一步”。

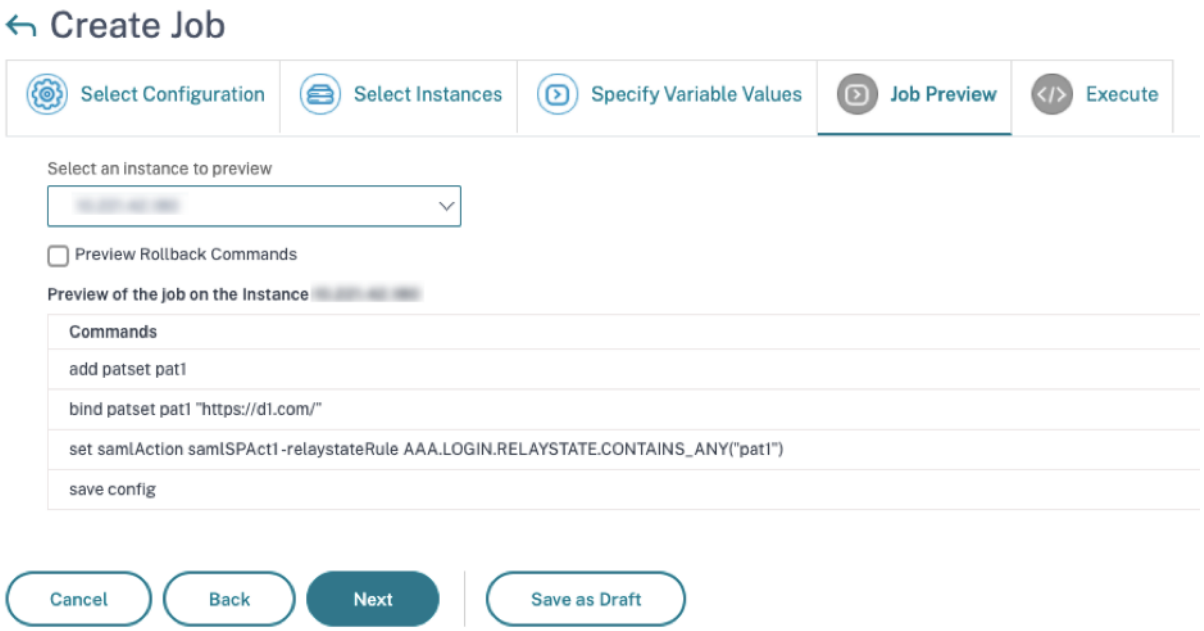


步骤 **3**：指定变量值　输入变量值。

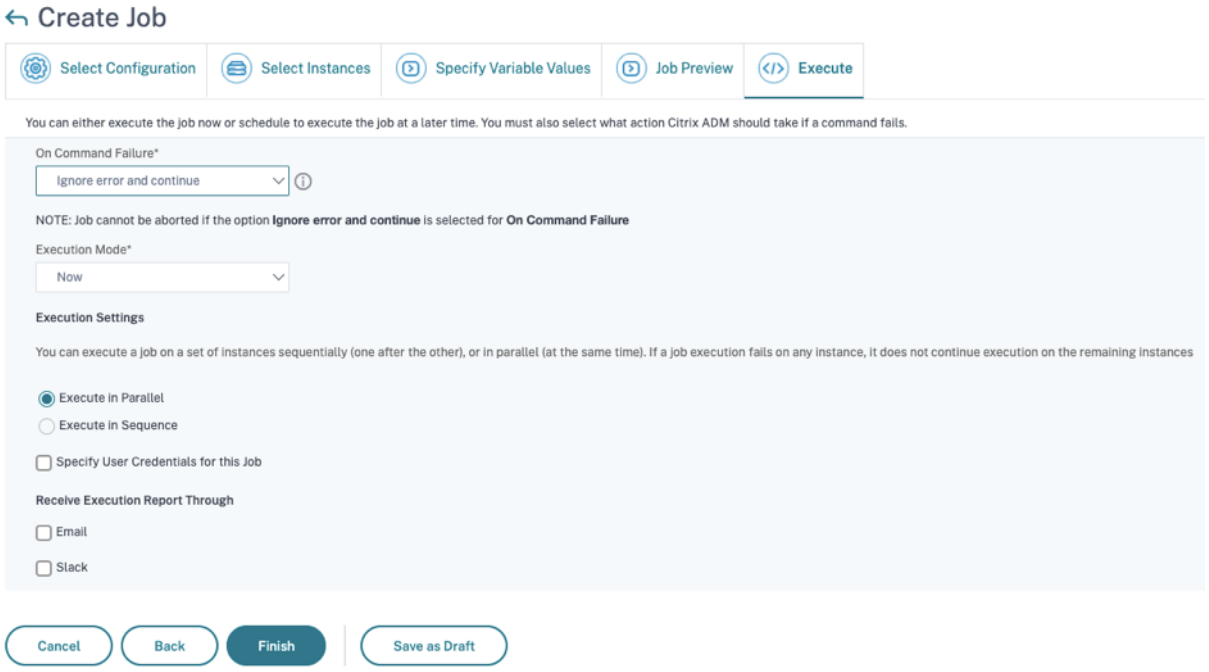
- `saml_action_patset`：为 SAML 操作添加一个名称
- `saml_action_domain1`：按 `https://<example1.com>/` 格式输入域名
- `saml_action_name`：输入与您为其配置作业的 SAML 操作相同的内容



步骤 **4**：预览配置　预览配置中已插入的变量值，然后单击“下一步”。



步骤 **5**：运行作业　单击“完成”运行配置作业。



作业运行后，它会显示在 基础结构 **>** 配置 **>** 配置作业下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修改后的安全状况。

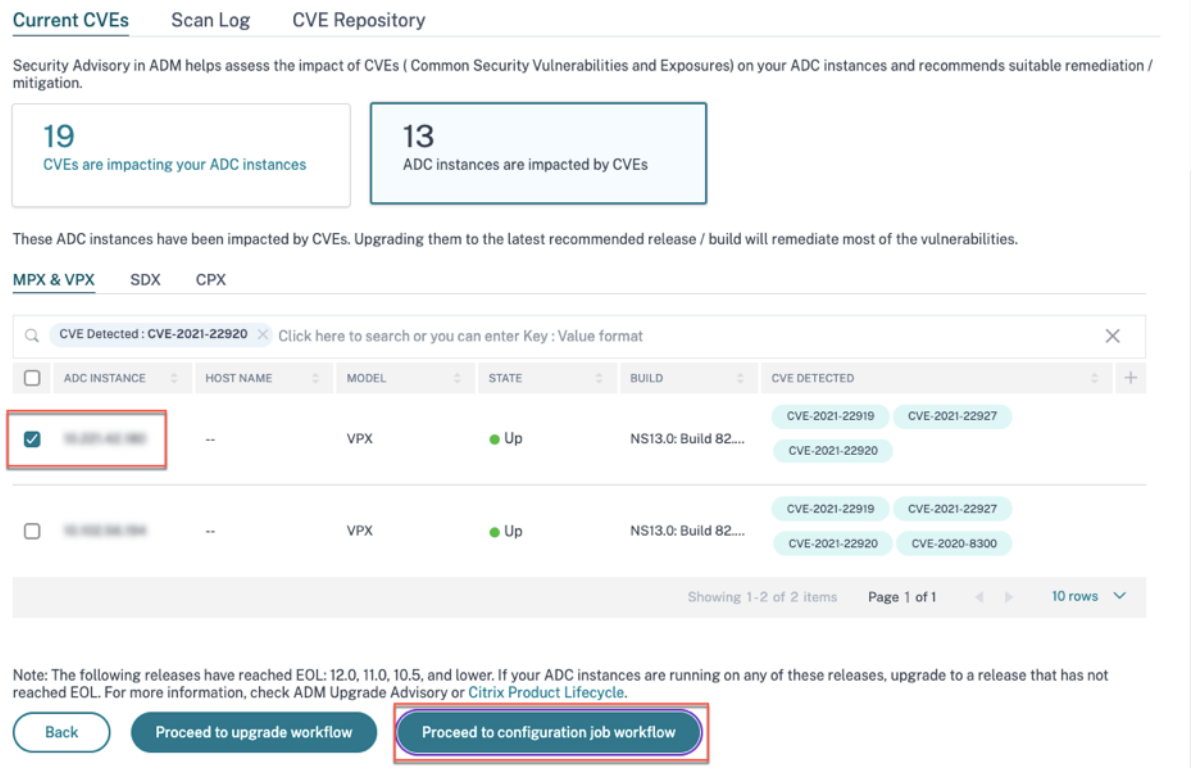
场景

在这种情况下，两个 NetScaler 实例易受 CVE-2021-22920 攻击，您需要修复所有实例。请按照以下步骤进行操作：

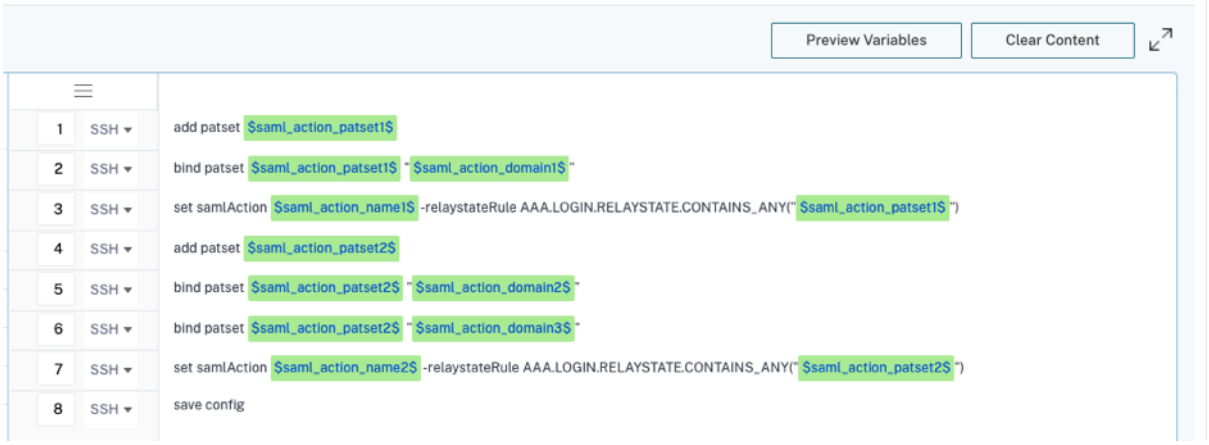
1. 按照本文档“升级实例”部分中给出的步骤，升级所有三个 NetScaler 实例。
2. 使用配置作业流程，一次将配置补丁应用到一个 NetScaler 上。请参阅本文档“应用配置命令”部分中给出的步骤。

易受攻击的 NetScaler 1 有两个 SAML 操作：

- SAML 操作 1 有一个域
- SAML 操作 2 有两个域



选择 NetScaler 1，然后 单击“继续配置作业流程”。内置基础模板会自动填充。接下来，给出作业名称并根据给定的配置自定义模板。

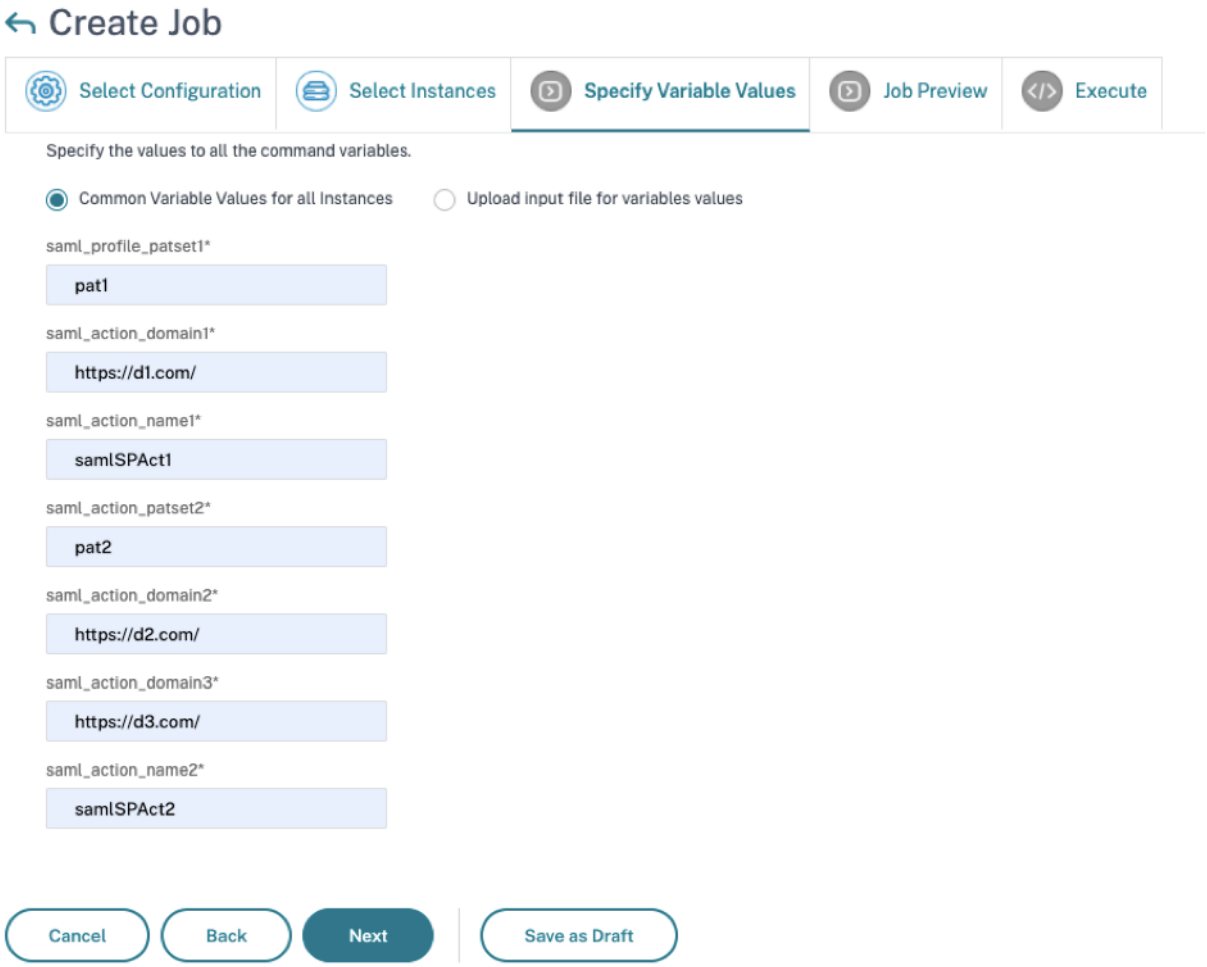


下表列出了自定义参数的变量定义。

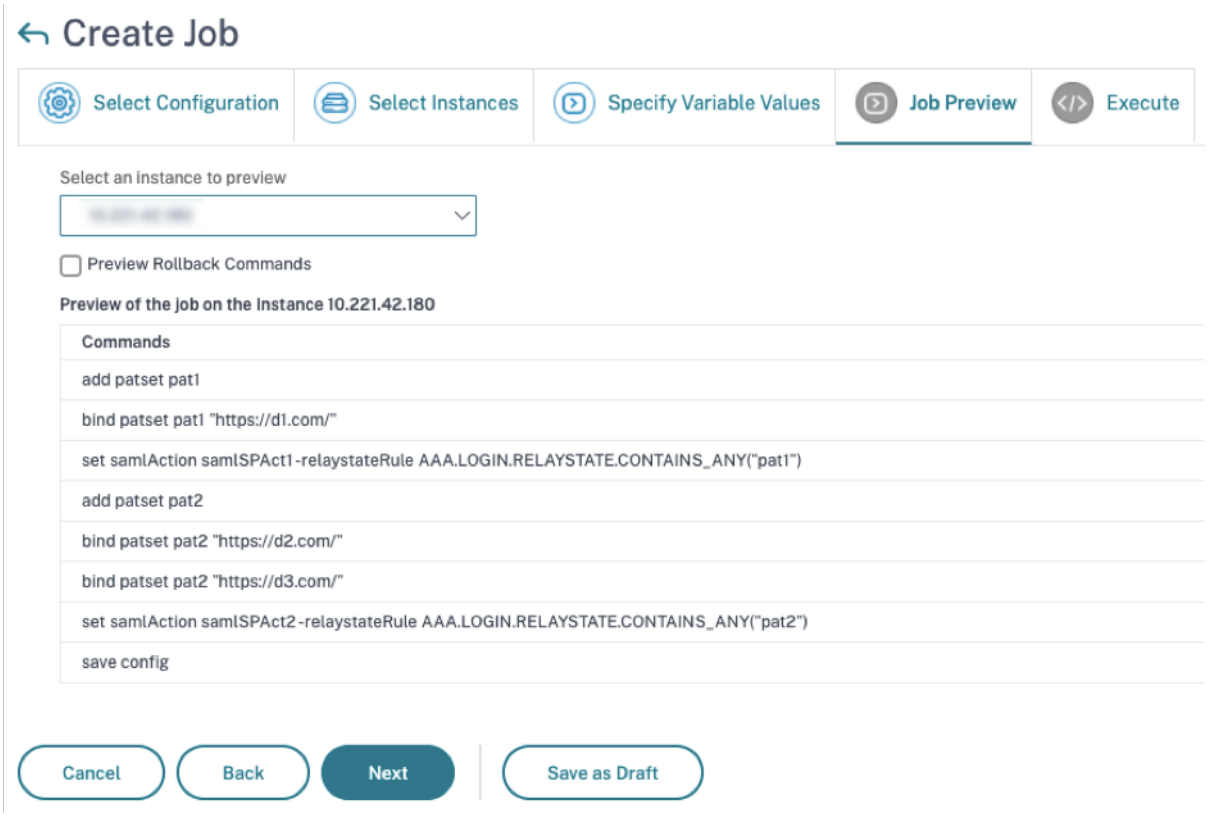
表。SAML 操作的变量定义

NetScaler 配置	patset 的变量定义	SAML 操作名称的变量定义	域的变量定义
SAML 操作 1 有一个域	saml_action_patset1	saml_action_name1	saml_action_domain1
SAML 操作 2 有两个域	saml_action_patset2	saml_action_name2	saml_action_domain2、saml_action_domain3

在“选择实例”下，选择 NetScaler 1，然后单击“下一步”。将出现“指定变量值”窗口。在此步骤中，您需要为上一步中定义的所有变量提供值。



接下来，查看变量。



单击“下一步”，然后单击“完成”以运行作业。

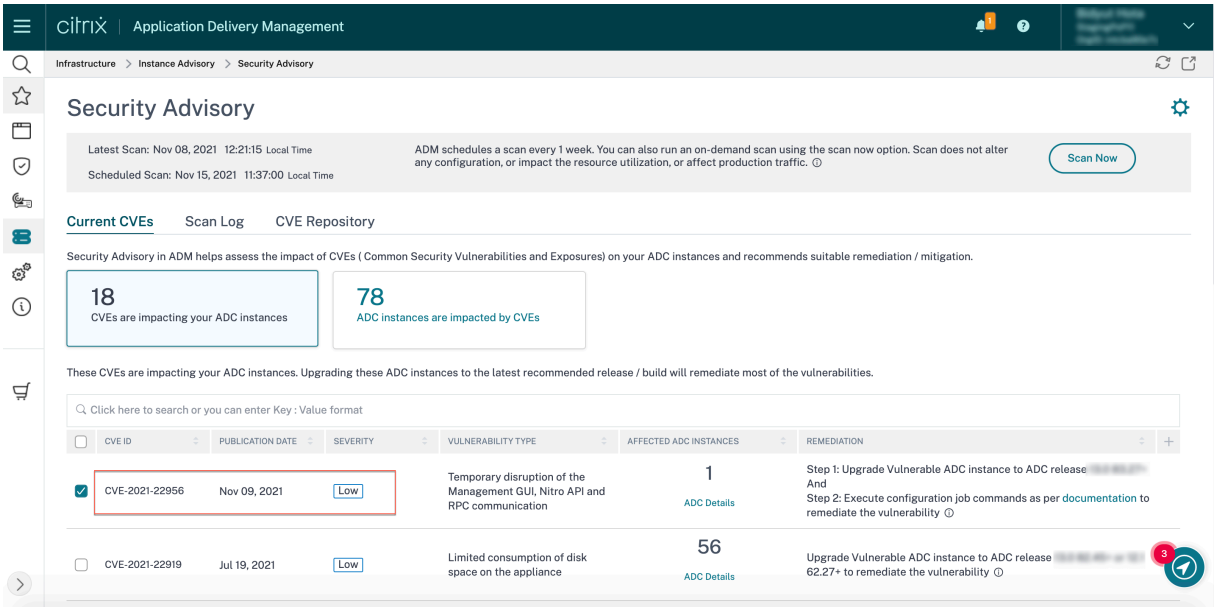
作业运行后，它会显示在 基础结构 **>** 配置 **>** 配置作业下。

完成 NetScaler 1 的两个修复步骤后，按照相同的步骤修复 NetScaler 2 和 NetScaler 3。修复完成后，您可以运行按需扫描以查看修改后的安全状态。

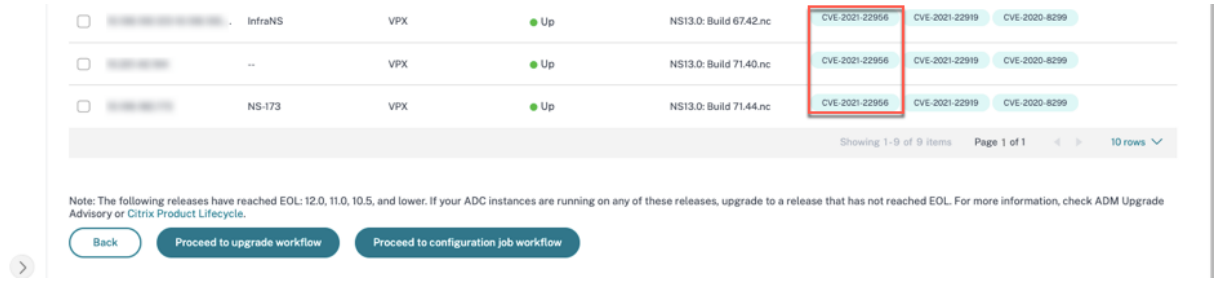
识别并修复 **CVE-2021-22956** 的漏洞

January 29, 2024

在 NetScaler 控制台安全公告控制面板中，在“当前 **CVE**”**>**“**<number of>**NetScaler 实例受常见漏洞和暴露 (CVE) 影响”下，您可以看到由于该特定 CVE 而易受攻击的所有实例。要查看受 CVE-2021-22956 影响的实例的详细信息，请选择 CVE-2021-22956，然后单击“查看受影响实例”。



将 <number of>出现受 CVE 影响的 NetScaler 实例窗口。在这里，您可以看到受 CVE-2021-22956 影响的 NetScaler 实例的数量和详细信息。



有关安全公告控制板的更多信息，请参阅安全公告。

> 注意
>
> 安全公告系统扫描可能需要一些时间才能得出结论并反映 CVE-2021-22956 在安全建议模块中的影响。要更快地查看影响，请单击“立即扫描”开始按需扫描。

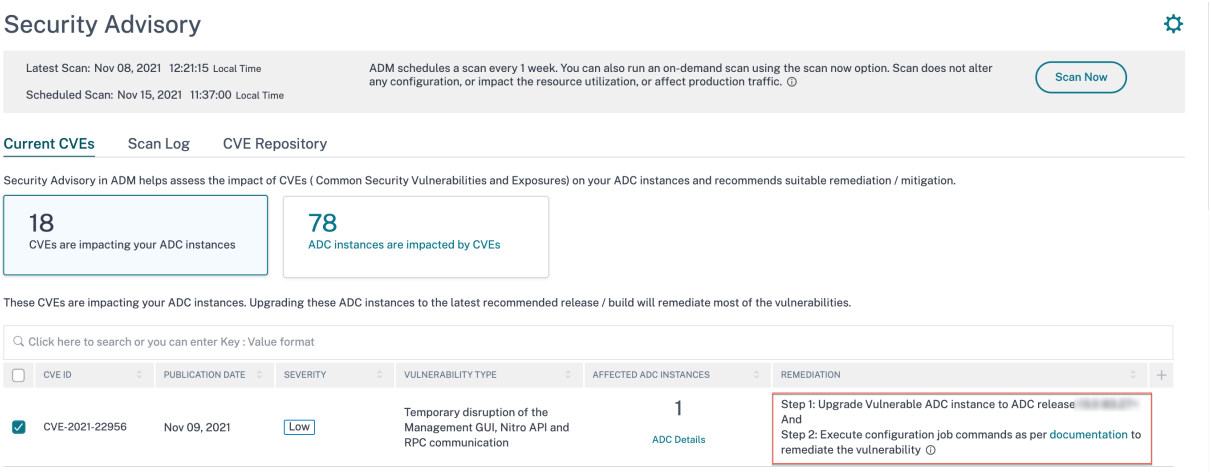
识别受 **CVE-2021-22956** 影响的实例

CVE-2021-22956 需要定制扫描，其中 NetScaler 控制台与托管的 NetScaler 实例连接并将脚本推送到该实例。该脚本在 NetScaler 实例上运行，并检查 Apache 配置文件 (`httpd.conf file`) 和最大客户端连接数 (`maxclient`) 参数，以确定实例是否存在漏洞。该脚本与 NetScaler 控制台共享的信息是布尔值（真或假）的漏洞状态。该脚本还向 NetScaler 控制台返回了不同网络接口（例如本地主机、NSIP 和具有管理访问权限的 SNIP）的 max_clients 计数列表。您可以在 CSV 文件中看到该列表的详细报告，您可以从“安全公告”页面的“扫描日志”选项卡下载该文件。

每次运行预定的按需扫描时，此脚本都会运行。扫描完成后，该脚本将从 NetScaler 实例中删除。

修复 **CVE-2021-22956**

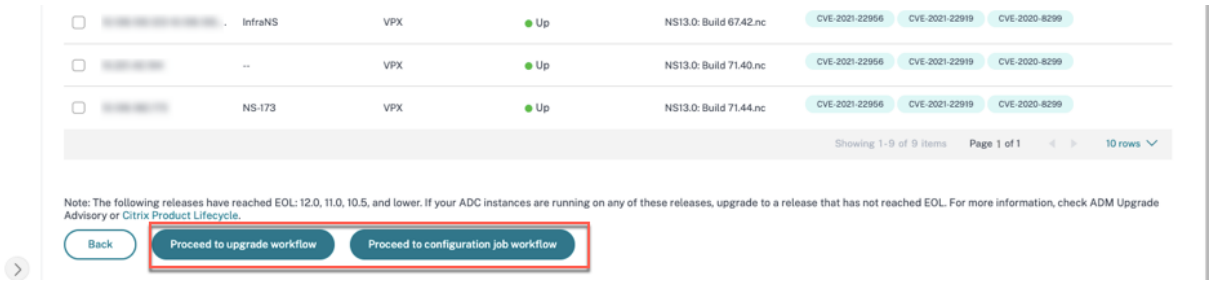
对于受 CVE-2021-22956 影响的 NetScaler 实例，补救过程分为两步。在 GUI 中，在“当前 CVE”**>** “**NetScaler** 实例受 CVE 影响”下，您可以看到第 1 步和第 2 步。



这两个步骤包括：

1. 将易受攻击的 NetScaler 实例升级到具有修复程序的版本和版本。
2. 在配置作业中使用可自定义的内置配置模板应用所需的配置命令。

在“当前 CVE> 受 CVE 影响的 NetScaler 实例”下，您可以看到此两步修复过程的两个独立工作流程：继续升级工作流程和继续配置作业工作流程。



第 **1** 步：升级易受攻击的 **NetScaler** 实例

要升级有漏洞的实例，请选择实例，然后单击“继续”升级工作流程。升级流程在已填充易受攻击的 NetScaler 实例的情况下打开。

有关如何使用 NetScaler 控制台升级 NetScaler 实例的详细信息，请参见创建 NetScaler 升级任务。

> 注意
>
> 对于所有易受攻击的 NetScaler 实例，可以立即执行此步骤。

步骤 **2**：应用配置命令

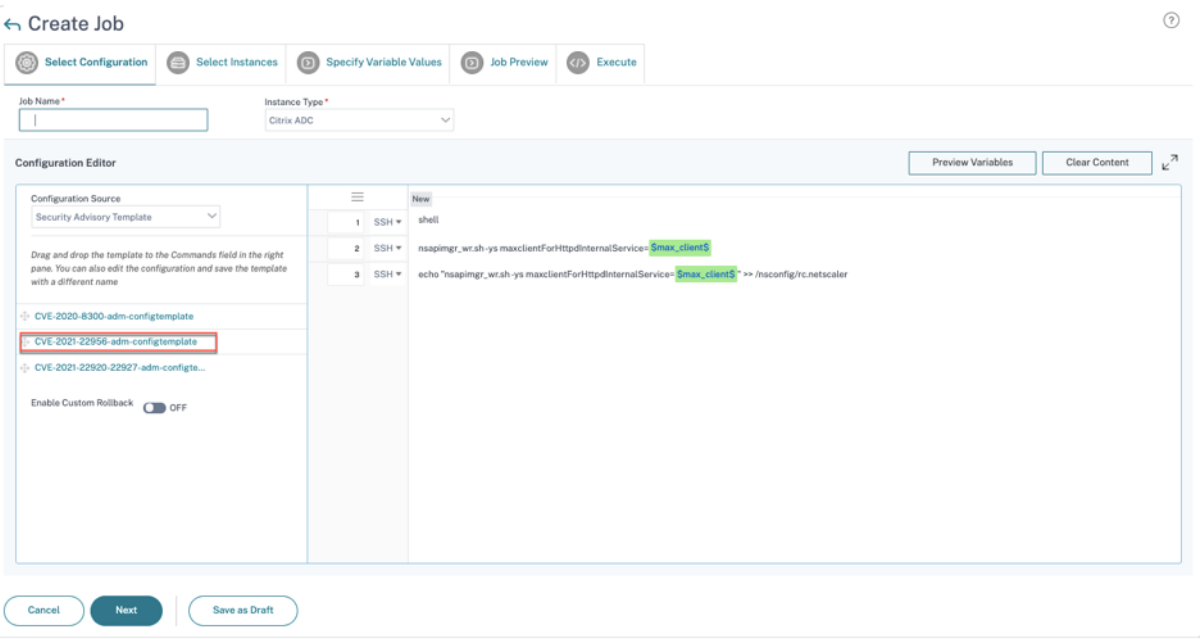
升级受影响的实例后，在 **<number of>** 受 **CVE** 影响的 **NetScaler** 实例窗口中，选择受 CVE-2021-22956 影响的实例，然后 单击继续配置作业流程。该工作流程包括以下步骤。

1. 自定义配置。
2. 查看自动填充的受影响实例。
3. 为作业的变量指定输入。
4. 查看填充变量输入的最终配置。
5. 运行作业。

在选择实例并单击“继续配置作业工作流程”之前，请记住以下几点：

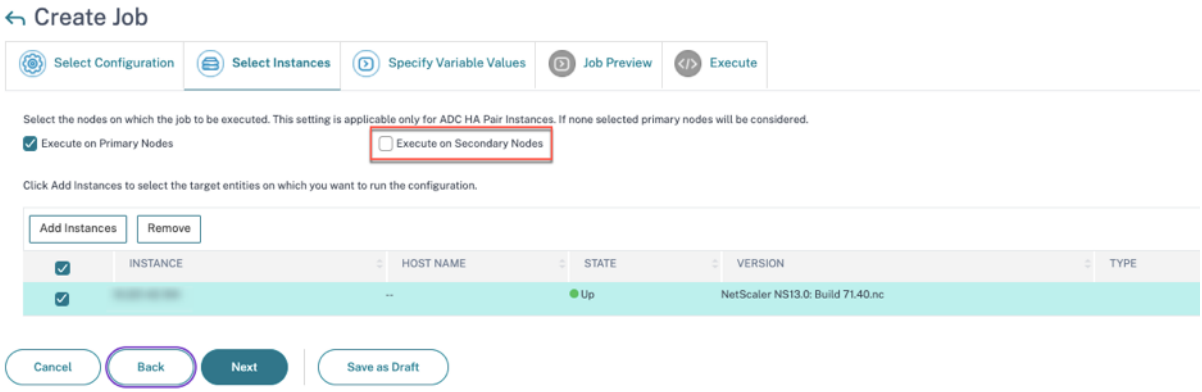
- 对于受多个 CVE（例如 CVE-2020-8300、CVE-2021-22927、CVE-2021-22920 和 CVE-2021-22956）影响的 NetScaler 实例：当您选择该实例并 单击“继续进行配置作业工作流程”时，内置配置模板不会自动填充在“选择配置”下。手动将安全公告模板下的相应配置作业模板拖放到右侧的配置作业窗格中。
- 对于仅受 CVE-2021-22956 影响的多个 NetScaler 实例：您可以同时在所有实例上运行配置作业。例如，您有 NetScaler 1、NetScaler 2 和 NetScaler 3，它们都只受到 CVE-2021-22956 的影响。选择所有这些实例，然后单击“继续配置作业工作流程”，内置配置模板将自动填充在“选择配置”下。请参阅 发行说明中的已知问题 NSADM-80913。
- 对于受 CVE-2021-22956 影响的多个 NetScaler 实例以及一个或多个其他 CVE（例如 CVE-2020-8300、CVE-2021-22927 和 CVE-2021-22920），这些实例需要同时对每个 NetScaler 进行补救：当您选择这些实例并 单击“继续配置作业流程”时，会出现一条错误消息，提示您一次在每个 NetScaler 上运行配置作业。

步骤 **1**：选择配置　在配置作业工作流中，内置配置基础模板会自动填充在“选择配置”下。



步骤 **2**：选择实例

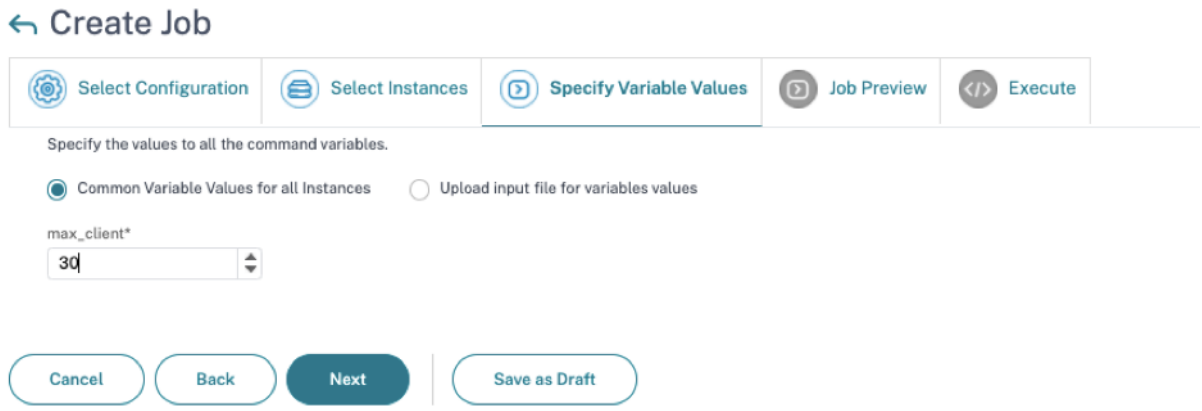
受影响的实例会在“选择实例”下自动填充。选择实例。如果此实例是 HA 对的一部分，请选择“在辅助节点上执行”。单击“下一步”。



> 注意
>
> 对于群集模式下的 NetScaler 实例，使用安全公告，NetScaler 控制台仅支持在群集配置协调器 (CCO) 节点上运行配置作业。在非 CCO 节点上单独运行命令。

在所有 HA 和群集节点上同步 `rc.netscaler`，使修复在每次重启后持续存在。

步骤 **3**：指定变量值　输入变量值。



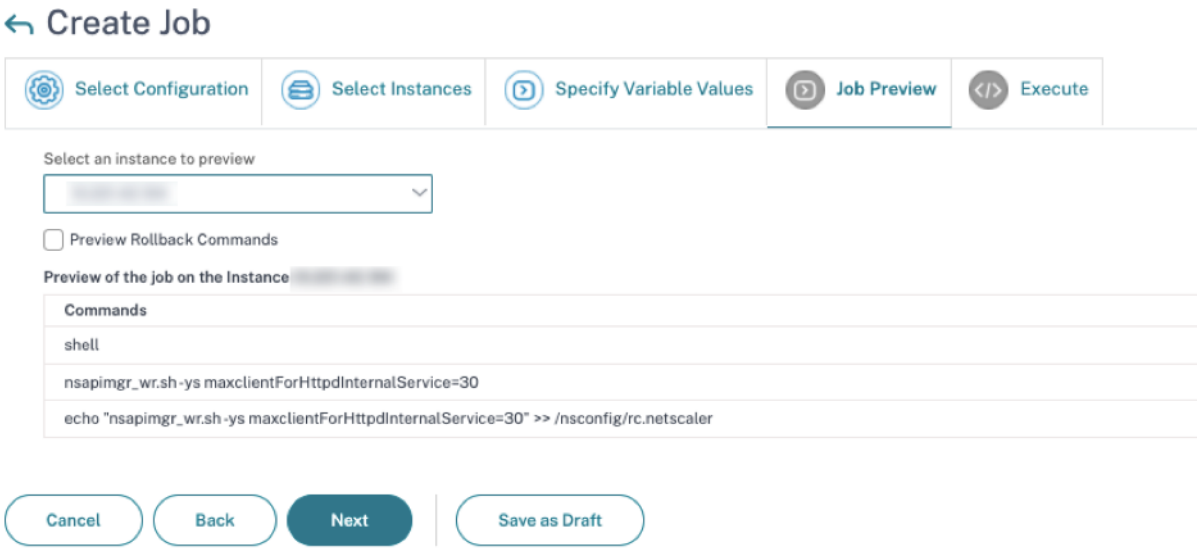
选择以下选项之一为您的实例指定变量：

所有实例的常用变量值：输入变量 `max_client` 的通用值。

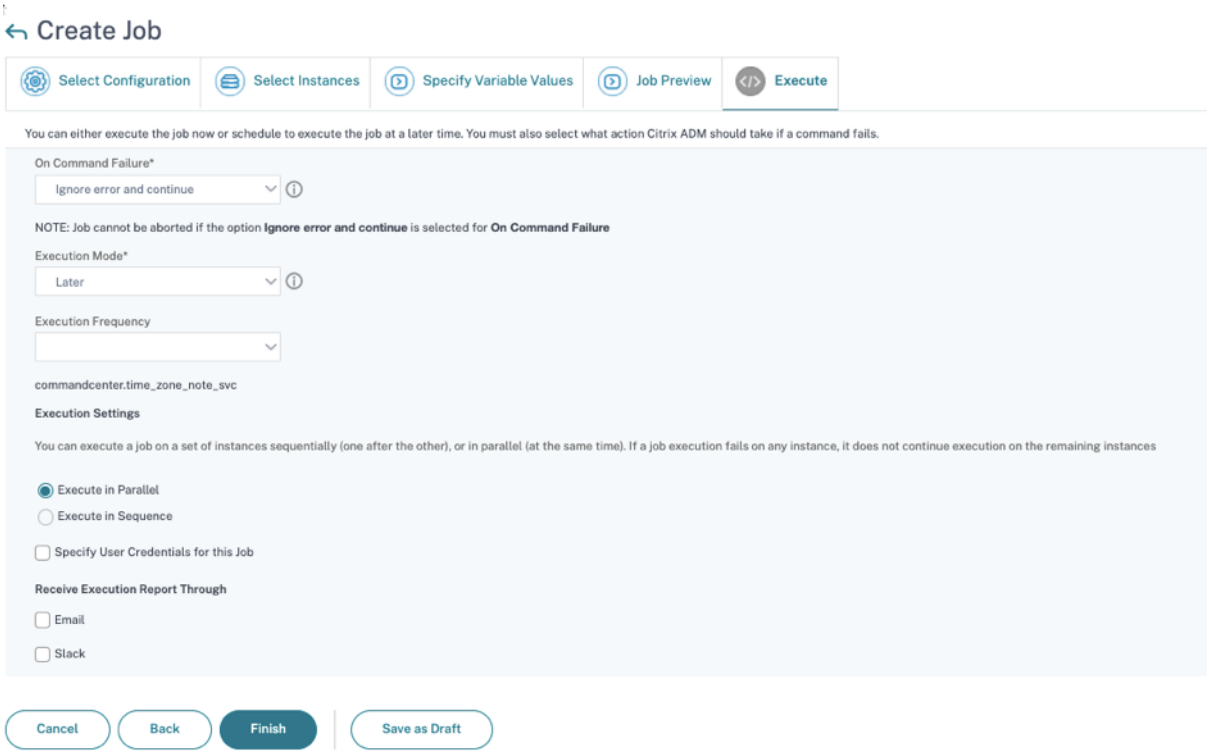
上载变量值的输入文件：单击“下载输入密钥文件”以下载输入文件。在输入文件中，输入变量的值`max_client`，然后将文件上载到 NetScaler 控制台服务器。有关此选项的问题，请参阅 发行说明 中的已知问题 NSADM-80913。

> 注意
>
> 对于上述两个选项，建议 `max_client` 值均为 30。您可以根据您的当前值设置该值。但是，它不应为零，并且应小于或等于 `/etc/httpd.conf` 文件中设置的 max_client。您可以 通过在 NetScaler 实例中搜索字符串 `MaxClients`，检查在 Apache HTTP Server 配置`/etc/httpd.conf`文件中设置的当前值

步骤 **4**：预览配置　预览配置中已插入的变量值，然后单击“下一步”。



步骤 **5**：运行作业　单击“完成”运行配置作业。



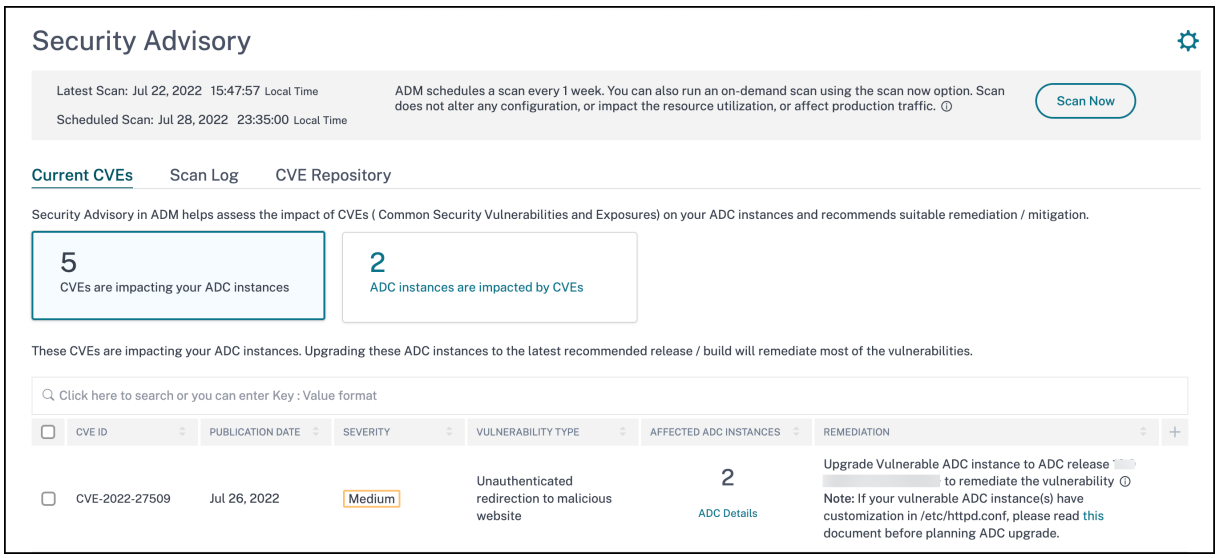
作业运行后，它会显示在 基础结构 **>** 配置 **>** 配置作业下。

完成所有易受攻击的 NetScaler 实例的两个修复步骤后，您可以运行按需扫描以查看修改后的安全状况。

识别并修复 **CVE-2022-27509** 的漏洞

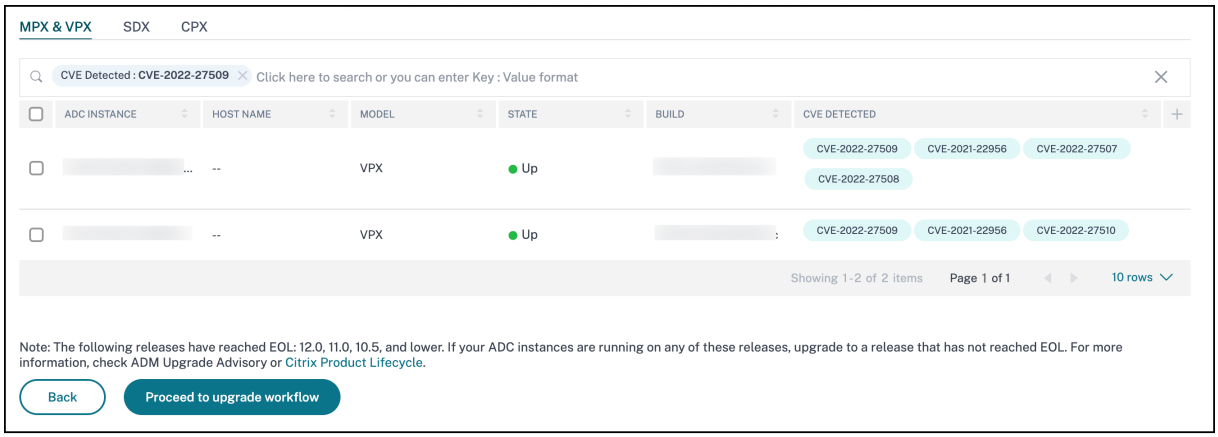
January 29, 2024

在 NetScaler 控制台安全公告控制面板中，在 “当<number of>前 CVE **NetScaler** 实例受到 CVE 影响” 下，您可以看到所有因 CVE-2022-27509 而易受攻击的实例。要查看受 CVE 影响的实例的详细信息，请选择 CVE-2022-27509，然后单击 “查看受影响的实例”。



> 注意
>
> 要了解 NetScaler 漏洞的原因，请在“安全公告”的“扫描日志”标签中下载 CSV 报告。

将出现**<number of>受 CVE 影响的 NetScaler** 实例窗口。在以下屏幕截图中，您可以看到受 CVE-2022-27509 影响的 NetScaler 实例的数量和详细信息。



有关安全公告控制板的更多信息，请参阅安全公告。

> 注意
>
> 安全警报系统扫描可能需要几个小时才能得出结论并反映 CVE-2022-27509 在安全公告模块中的影响。要更快地查看影响，请单击“立即扫描”开始按需扫描。

识别受 **CVE-2022-27509** 影响的实例

CVE-2022-27509 需要将自定义扫描和版本扫描相结合。作为定制扫描的一部分，NetScaler 控制台与托管的 NetScaler 实例连接，并将脚本推送到该实例。该脚本在 NetScaler 实例上运行并确定该实例是否存在漏洞。每次运行预设扫描或按需扫描时，此脚本都会运行。

扫描完成后，该脚本将从 NetScaler 实例中删除。

您也可以选择退出这些安全公告自定义扫描。有关自定义扫描设置和选择退出自定义扫描的更多信息，请参阅“安全公告”页面上的“配置自定义扫描设置”部分。

修复 **CVE-2022-27509**

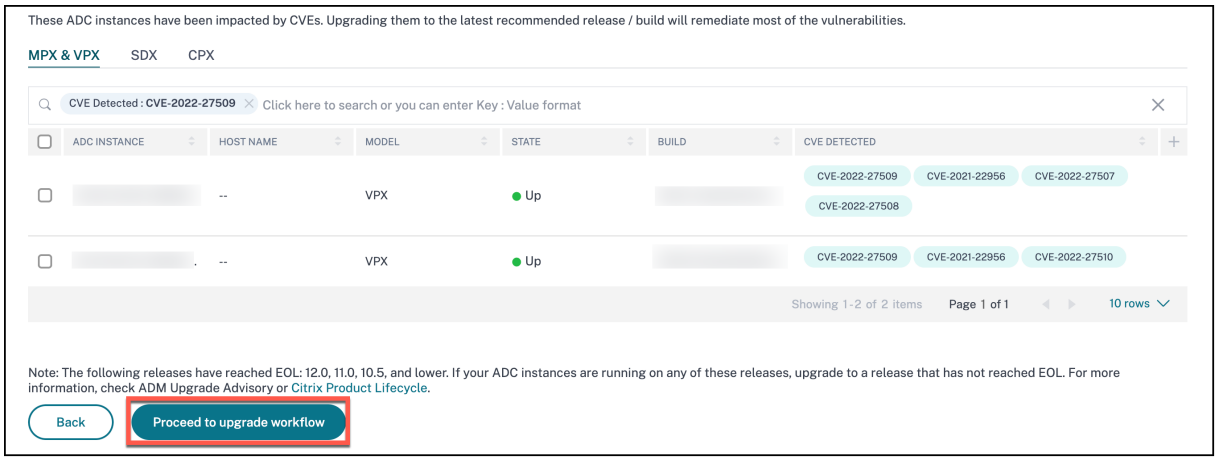
对于受 CVE-2022-27509 影响的 NetScaler 实例，修复是一个单步过程，您需要将易受攻击的 NetScaler 实例升级到具有修复功能的版本和版本。在 GUI 中，在“当前 CVE”**>** “**NetScaler** 实例受 CVE 影响”下，您可以看到修复步骤。

在“当前 **CVE>** 受 **CVE** 影响的 **NetScaler** 实例”下，您可以看到此单步修复过程的以下工作流程，即“继续升级流程”。

要升级有漏洞的实例，请选择实例，然后单击“继续”升级工作流程。升级流程在已填充易受攻击的 NetScaler 实例的情况下打开。

> 重要
>
> 如果您的易受攻击的 NetScaler 实例已将 /etc/httpd.conf 文件复制到 /nsconfig 目录，请在规划 NetScaler 升级之前，参见自定义 NetScaler 配置的升级注意事项。

有关如何使用 NetScaler 控制台升级 NetScaler 实例的详细信息，请参见创建 NetScaler 升级任务。



安全公告中不支持的 **CVE**

January 29, 2024

NetScaler 控制台安全公告跟踪所有新的常见漏洞和暴露 (CVE)，并评估 CVE 对基础架构的影响。您可以查看建议并采取适当的措施。但是，有几个 CVE 不受支持，漏洞的检测和修复超出了 NetScaler 控制台安全公告的范围。

- **CVE-2022-21827**:

  CVE-2022-21827 会影响 21.9.1.2 之前支持的 Windows 版本的 NetScaler Gateway 插件。

  NetScaler 控制台不支持检测和修复影响适用于 Windows 的 NetScaler Gateway 插件的漏洞。此外，无法通过在 NetScaler 端执行任何检查、验证 NetScaler 版本或检查 NetScaler 配置来评估 NetScaler Gateway 插件漏洞。此 CVE 的检测和修复只能根据客户端上部署的适用于 Windows 的 NetScaler Gateway 插件版本进行评估。

  因此，对该漏洞的检测和修复超出了 NetScaler 控制台安全公告的范围。

设置

January 29, 2024

初始设置完成后，必须配置某些设置才能开始完全管理部署。

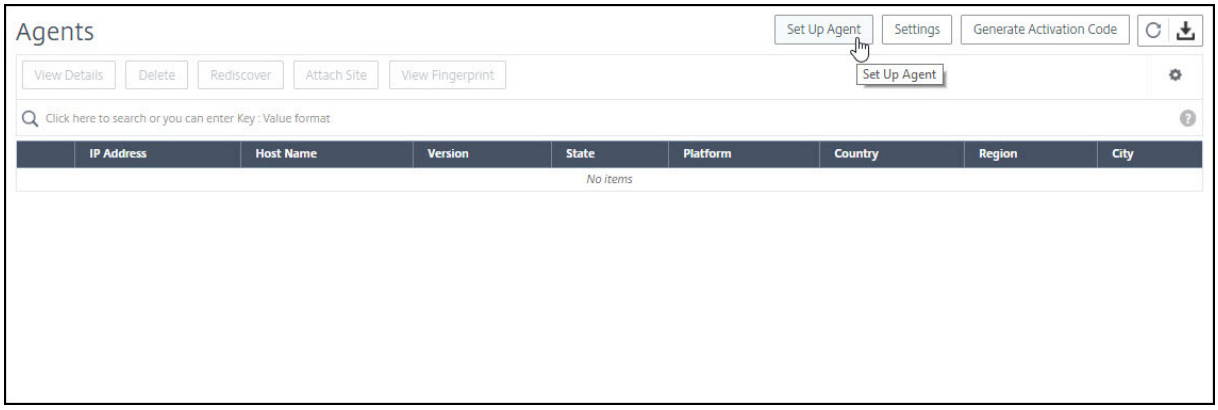
- 添加多个代理。要安装的代理数量取决于数据中心或云中的托管实例数量和总吞吐量。Citrix 建议您为每个数据中心至少安装一个代理。
- 添加实例。您可以在 首次设置 NetScaler 控制台时添加实例，也可以在以后 添加实例。您必须向服务添加实例才能开始管理和监视它们。安装多个代理后，必须添加实例并将其与代理关联。
- 启用分析。要查看应用程序通信流的分析数据，必须在接收特定应用程序的流量的虚拟服务器上启用分析功能。
- 在实例上配置系统日志。如果您已将设备配置为将所有系统日志消息重定向到 NetScaler 控制台，则可以监视在 NetScaler 实例上生成的系统日志事件。要监视系统日志事件，首先需要将 NetScaler 控制台配置为 NetScaler 实例的系统日志服务器。
- 配置基于角色的访问控制。NetScaler 控制台提供精细的、基于角色的访问控制 (RBAC)，您可以根据企业内个人用户的角色授予访问权限。
- 配置分析设置。您可以配置某些设置，以确保使用 Analytics 功能获得最佳体验。例如，您可以指定存储历史分析数据的持续时间，也可以设置阈值和警报以监视所需的分析指标。

添加多个代理

January 29, 2024

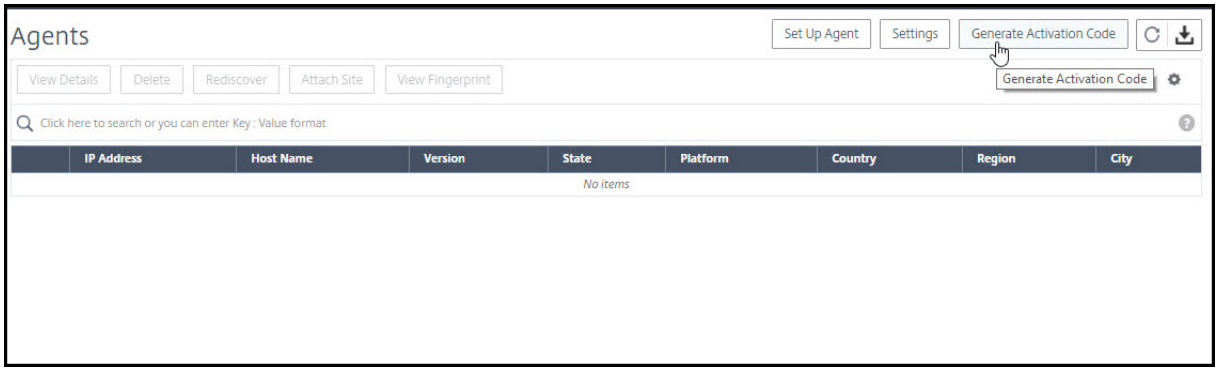
要安装的代理数量取决于数据中心中托管实例的数量和总吞吐量。Citrix 建议您为每个数据中心至少安装一个代理。

首次登录该服务时，只能安装一个代理。要添加多个代理，请先完成初始设置，然后导航到 基础结构 **>** 实例 **>** 代理，然后单击 设置代理。



下载所需虚拟机管理程序的映像，然后按照 入门中的说明安装代理。 请务必复制屏幕上显示的服务 URL 和激活码，因为在虚拟机管理程序上安装代理时必须输入服务 URL 和激活码。代理使用服务 URL 查找服务，并使用激活代码向服务注册。

您可以使用同一个映像在虚拟机管理程序中安装多个代理。但是，您不能在多个代理上使用相同的激活码。安装一个代理后，再次为下一个代理生成激活码。您可以通过导航到 基础结构 > 实例 > 代理，单击“生成激活码”来生成新的激活码。



成功安装和注册代理后，验证服务 GUI 上的代理状态并向其添加实例。

> 注意
>
> 您也可以在 Microsoft Azure 云或 AWS 云上安装代理。客户端映像在相应的云市场上可用。
>
> - 有关在 Microsoft Azure 云上安装代理的说明，请参阅在 Microsoft Azure 云上安装 NetScaler 代理。
> - 有关在 AWS 上安装代理的说明，请参见在 AWS 上 安装 NetScaler代理。

为多站点部署配置代理

January 29, 2024

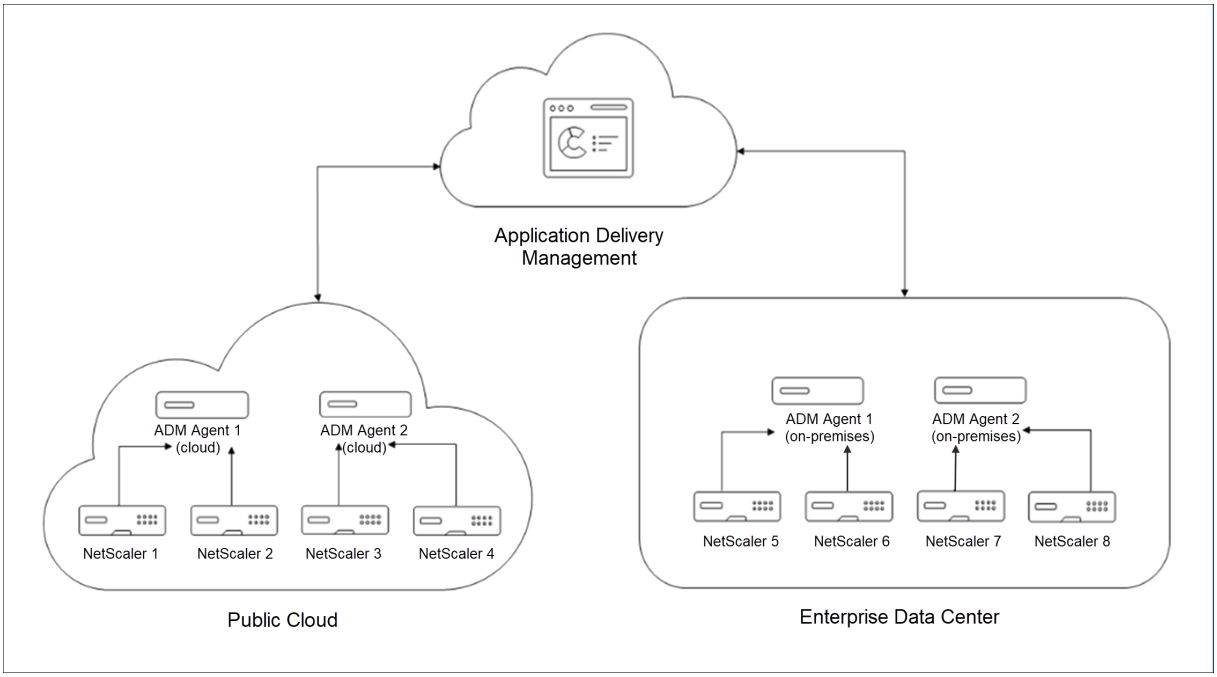
代理充当 NetScaler 控制台与跨不同数据中心和公有云发现的实例之间的中介。NetScaler 控制台支持在数据中心或公有云内进行代理故障转移。

以下是安装代理的好处：

- 代理的配置实例将未处理的数据直接发送到代理，而不是 NetScaler 控制台。代理进行第一级数据处理，并将经过处理的数据以压缩格式发送到 NetScaler 控制台进行存储。
- 代理和实例位于同一数据中心或云中，以便更快地处理数据。
- 对代理进行群集可在代理故障转移时重新分配 NetScaler 实例。当站点中的一个代理出现故障时，来自 NetScaler 实例的流量会切换到同一站点中的另一个可用代理。

体系结构

下图说明了在数据中心和公共云中的多个代理上配置的 NetScaler 实例，以实现代理故障转移：



公有云有四个 NetScaler 实例和两个代理。企业数据中心还有四个 NetScaler 实例和两个 代理。每个代理都配置了两个 NetScaler 实例。

代理直接从配置的实例接收数据。代理收到数据后，代理处理数据并以压缩格式发送到 NetScaler 控制台。代理通过安全通道与 NetScaler 控制台服务器通信。

在公有云上，当 代理 **1** 变为非活动状态（关闭状态）时，会发生代理故障转移。NetScaler 控制台使用代理 **2** 重新分发代理 **1** 的 NetScaler 实例。如果其中一个代理在数据中心出现故障，则实例重新分配将在企业数据中心上进行。

要安装代理，请参见 安装 NetScaler代理。

代理故障转移

代理故障切换可能发生在具有两个或多个注册代理的站点中。当站点中的代理处于非活动状态（关闭状态）时，NetScaler 控制台会将该非活动代理的 NetScaler 实例与其他活动代理一起重新分发。

> 重要
>
> - 代理故障转移不考虑 CPX 实例。
> - 确保您的帐户上已启用代理故障转移功能。要启用此功能，请参见 启用或禁用 NetScaler 控制台功能。
> - 如果代理正在运行脚本，请确保该脚本存在于站点中的所有代理上。因此，更改的代理可以在代理故障转移后运行脚本。

要在 NetScaler 控制台 GUI 中将站点连接到代理，请执行以下操作：

1. 导航到 基础结构 **>** 实例 **>** 代理。
2. 选择要连接到站点的代理。
3. 从列表中指定站点。如果要添加新站点，请单击 添加。
4. 单击保存。

要实现代理故障转移，请逐一选择代理并连接到同一个站点。

例如，两个代理 10.106.1xx.2x 和 10.106.1xx.7x 已连接并在班加罗尔站点运行。如果一个代理处于非活动状态，NetScaler 控制台会检测到该代理并将其状态显示为关闭。

当站点中的代理处于非活动状态（关闭状态）时，NetScaler 控制台会等待几分钟让该代理变为活动状态（启动状态）。如果代理处于非活动状态，NetScaler 控制台会自动在同一站点的可用代理之间重新分配实例。此重新分发可能需要大约 10-15 分钟。

NetScaler 控制台每 30 分钟触发一次实例再分配，以平衡站点中活跃代理之间的负载。

连接并自动重新配置到同一站点中的代理的实例，以进行陷阱目标、syslog 服务器和分析。

配置代理升级设置

January 29, 2024

在 NetScaler 控制台中，运行在软件版本 12.0 build 507.110 及更高版本上的代理会由 NetScaler 控制台自动升级到更新的推荐版本。有新版本可用时或在您指定的时间升级代理。

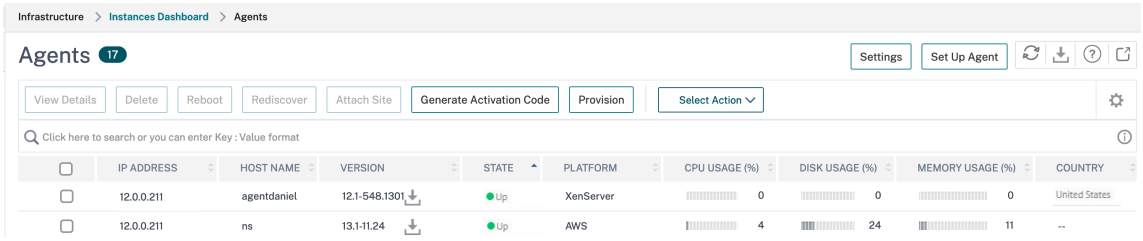
您可以导航到 基础结构 **>** 实例代理，查看代理的当前版本和推荐版本。

默认情况下，当较新版本可用时，代理会自动升级。但是，您可以为每个代理安排升级。

在升级期间，可能会有大约五分钟的停机时间。

要配置代理升级设置，请执行以下操作：

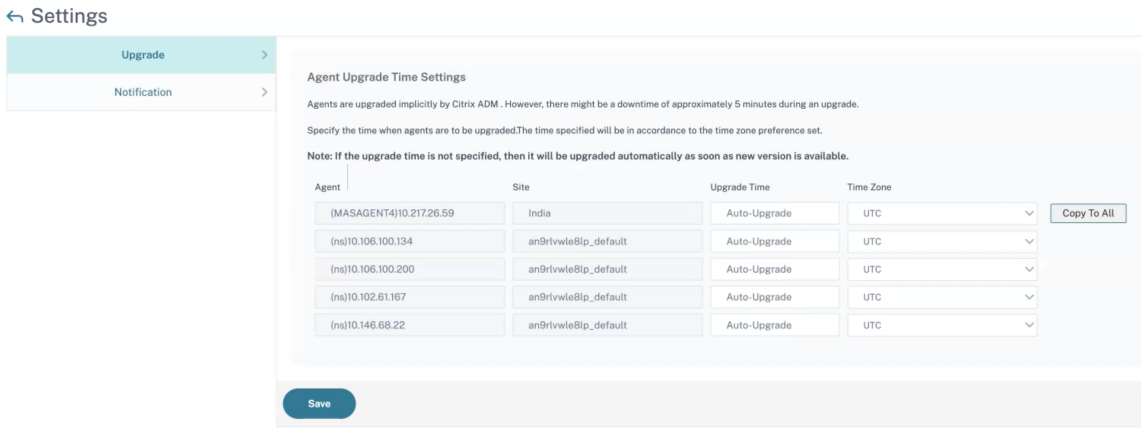
1. 导航到 基础结构 > 实例 > 代理，单击 设置。



2. 指定您希望何时开始每个代理的升级。

   您可以使用以下选项之一来升级代理：

   - 自动升级 - 选择自动升级，以便在新的代理映像可用时升级代理。如果未输入值，则默认情况下会选择“自动升级”。
   - 设置特定时间：输入时间（以 hh: mm 格式），然后选择希望 NetScaler 控制台自动升级代理的时区。



   您可以单击“复制到全部”将相同的升级时间应用到所有代理。

3. 单击保存。

   这些设置一直保留在将来的代理升级之前，直到您更改设置。

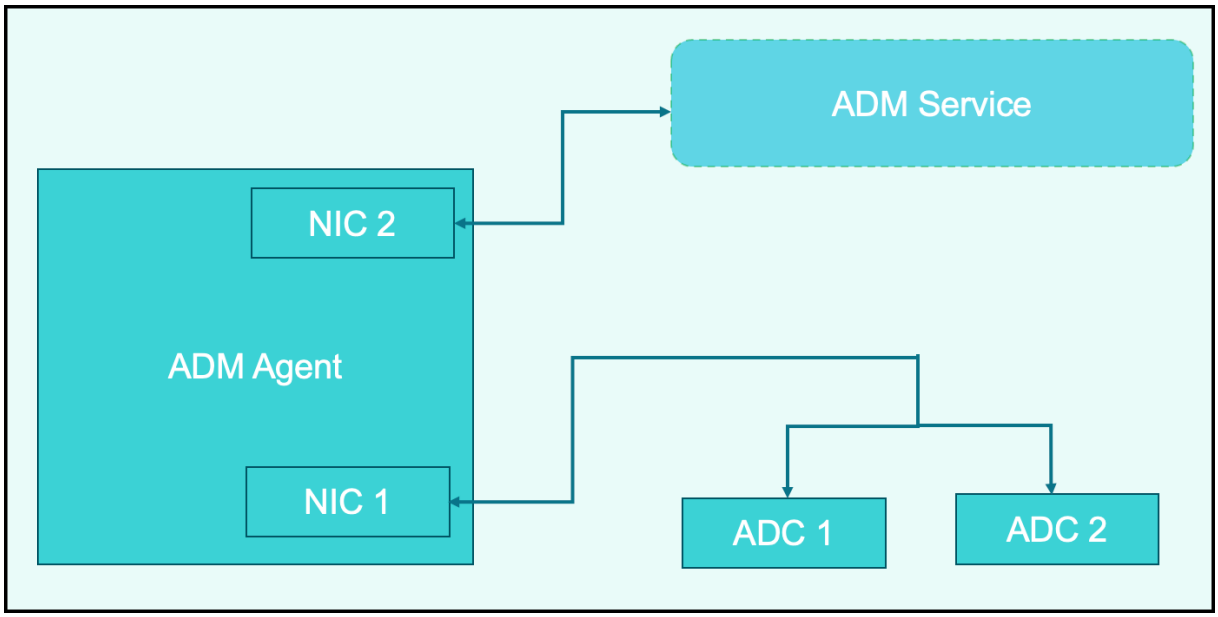
NetScaler 控制台支持双 NIC

January 29, 2024

您可以在代理上配置两个 NIC。使用双 NIC 架构，代理将能够：

- 在代理和 NetScaler 实例之间建立通信-您可以使用第一个 NIC 隔离通过 NetScaler 控制台接收和发送的流量，也可以在 NetScaler 控制台与其托管 NetScaler 实例之间进行通信。
- 在代理和 NetScaler 控制台之间建立通信-您可以使用第二个 NIC 来管理网络上的 NetScaler 控制台并执行管理任务。

> 注意
>
> 您无法互换两个 NICS 的功能和配置。



在这种情况下，作为管理员，您可以：

- 为 NetScaler 控制台与其托管 NetScaler 实例之间的流量配置 IP 地址。
- 配置 IP 地址以管理 NetScaler 控制台软件，以执行软件中的所有管理任务。

> 注意
>
> 不强制为代理配置双网卡。它是可选的，仅在需要分离代理、NetScaler 控制台服务和 NetScaler 实例之间的流量时才是必需的。

必备条件

- 确保您已在虚拟机管理程序（Citrix Hypervisor、Microsoft Hyper-V、Linux KVM 或 VMware ESXi）上部署和配置 NetScaler 代理。
- 确保已在 Hypervisor（Citrix Hypervisor、Microsoft Hyper-V、Linux KVM 或 VMware ESXi）上添加了第二个网卡。

要为 Citrix Hypervisor 上的 NIC 分配 IP 地址并创建辅助接口，请参阅 为 NIC 分配 IP 地址。

修改 IPV4 网卡网络地址

1. 使用 SSH 客户端（例如 PuTTY）打开与 NetScaler 代理控制台的 SSH 连接。
2. 使用 nsrec **over/nsroot** 凭据登录并切换到 shell 提示符。
3. 运行 **ifconfig** 命令。您可以看到已配置的两个 NIC 的详细信息-
   - NIC 1 —用于代理与 NetScaler 通信之间的通信
   - NIC 2 —用于代理和 NetScaler 控制台之间的通信

```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. 运行 n **etworkconfig** 命令。出现一个菜单，允许您设置或修改 IPV4 网络地址。

```
bash-3.2# /mps/networkconfig

------------------------------------------------------------------------------
Citrix ADM Agent initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
     1. Citrix ADM Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```


> 注意：
>
> 第二个 NIC 网络地址可以采用多个 IP 值。

5. 选择要修改的菜单项。保存并退出设置。

添加实例

January 29, 2024

您可以在 首次设置 NetScaler 控制台时添加实例，也可以在以后 添加实例。

实例是您想要从 NetScaler 控制台发现、管理和监视的 NetScaler 设备或虚拟设备。您可以将以下 NetScaler 设备和虚拟设备添加到 NetScaler 控制台：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway
- Citrix Secure Web Gateway

要添加实例，您必须指定每个 NetScaler 实例的主机名或 IP 地址，或指定 IP 地址范围。

指定 NetScaler 控制台可用于访问该实例的实例配置文件。此实例配置文件包含要添加到服务的实例的用户名和密码。对于每个实例类型，都有一个默认的配置文件。例如，ns-root-profile 是 NetScaler 实例的默认配置文件。默认 NetScaler 管理员凭据定义此配置文件。如果更改了实例的默认管理员凭据，可以为那些实例定义自定义实例配置文件。如果在发现实例后更改实例的凭据，则必须编辑实例配置文件或创建一个配置文件，然后重新发现实例。

在 NetScaler 控制台中添加实例后，您可以从 NetScaler 控制台访问这些实例的 GUI。要从 NetScaler 控制台访问 NetScaler 实例，必须连接到 Citrix 网络。

> 注意
>
> - 要添加在群集中配置的 NetScaler 实例，必须指定群集 IP 地址或群集设置中的任何一个单独节点。但是，在 NetScaler 控制台上，群集 IP 地址代表群集。
> - 对于设置为 HA 对的 NetScaler 实例，当您添加一个实例时，将自动添加对中的另一个实例。
> - 要确保 NetScaler 用户拥有所有权限，请在 NetScaler 中为该用户分配超级用户权限。有关更多信息，请参阅 用户、用户组和命令策略

如何创建 **NetScaler** 配置文件

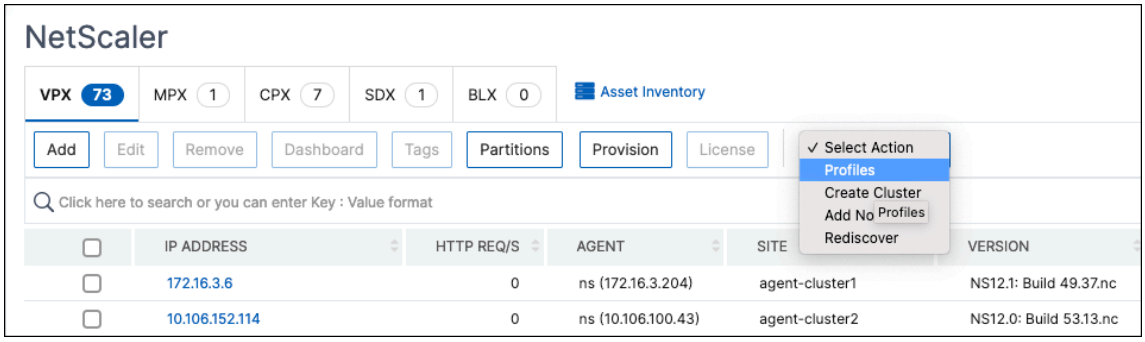
NetScaler 配置文件包含要添加到 NetScaler 控制台的实例的用户名、密码、通信端口和认证类型。对于每个实例类型，都有一个默认的配置文件。例如，`nsroot` 是 NetScaler 实例的默认配置文件。默认配置文件通过使用默认 NetScaler 管理员凭据来定义。如果更改了实例的默认管理员凭据，可以为那些实例定义自定义实例配置文件。如果在发现实例后更改实例的凭据，则必须编辑实例配置文件或创建一个配置文件，然后重新发现实例。

您可以从“实例”页面或在添加或更改实例 时创建 NetScaler 配置文件。

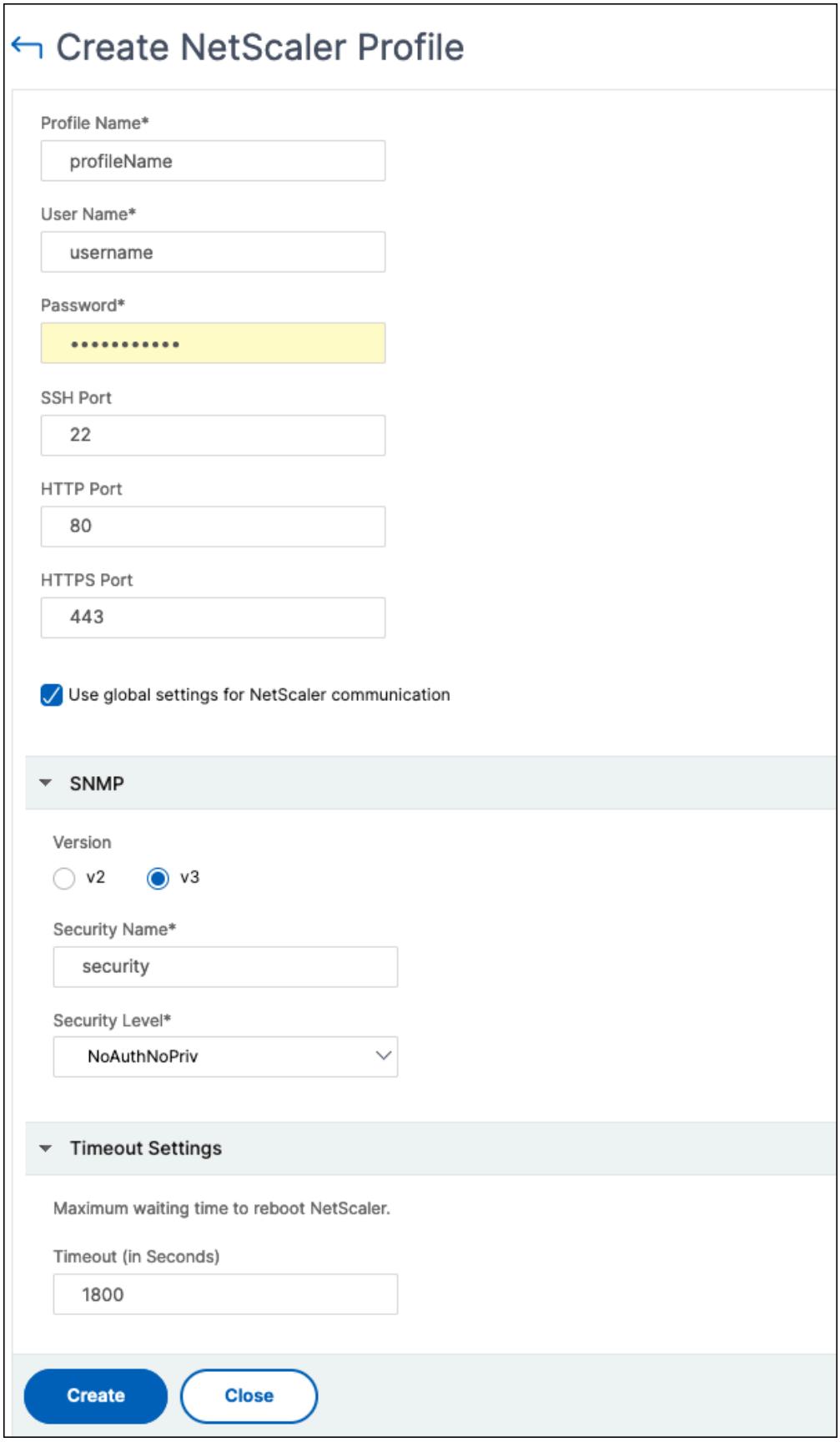
> 注意：
>
> 确保使用超级管理员帐户创建实例配置文件。

要从“实例”页创建 **NetScaler** 配置文件，请执行以下操作：

1. 导航到 **Infrastructure**（基础结构）**> Instances**（实例）。
2. 选择一个实例。例如，NetScaler。
3. 在 NetScaler 页面上的 选择操作 下，选择 配置文件。



4. 在“管理员配置文件”页面上，选择“添加”。
5. 在创建 **NetScaler** 配置文件页面上，执行以下操作：



a) 配置文件名称：为 NetScaler 实例指定配置文件名称。

b) 用户名：指定登录到 NetScaler 实例的用户名。

c) 密码：指定登录到 NetScaler 实例的密码。

d) **SSH** 端口：指定 NetScaler 控制台和 NetScaler 实例之间进行 SSH 通信的端口。

e) **HTTP** 端口：指定 NetScaler 控制台和 NetScaler 实例之间的 HTTP 通信端口。

> 注意：
>
> 默认 HTTP 端口为 80。您还可以指定可能在 NetScaler CPX 实例中配置的非默认或自定义 HTTP 端口。自定义的 HTTP 端口只能用于 NetScaler 控制台和 NetScaler CPX 之间的通信。

f) **HTTPS** 端口：指定 NetScaler 控制台和 NetScaler 实例之间的 HTTPS 通信端口。

> 注意：
>
> 默认 HTTPS 端口为 443。您还可以指定可能在 NetScaler CPX 实例中配置的非默认或自定义 HTTPS 端口。自定义的 HTTPS 端口只能用于 NetScaler 控制台和 NetScaler CPX 之间的通信。

g) 使用全局设置进行 **NetScaler** 通信：如果您想使用系统设置在 NetScaler 控制台和 NetScaler 实例之间进行通信，请选择此选项，否则请选择 HTTP 或 https。

h) **SNMP** 版本：选择 **SNMPv2** 或 **SNMPv3** ，然后执行以下操作：

i. 如果选择 SNMPv2，请指定用于身份验证的社区名称。

ii. 如果选择 SNMPv3，请指定安全名称和安全级别。根据安全级别，选择 身份验证类型 和 隐私类型。

> 注意：
>
> 对于 NetScaler SDX，仅支持 **SNMPv2**。

i) 超时设置：指定 NetScaler 控制台在重启后向 NetScaler 实例发送连接请求之前必须等待的时间。

j) 选择创建。

向 **NetScaler** 控制台添加 **NetScaler** 实例

> 注意
>
> 执行此任务以添加除 NetScaler CPX 实例之外的所有其他 NetScaler 实例。

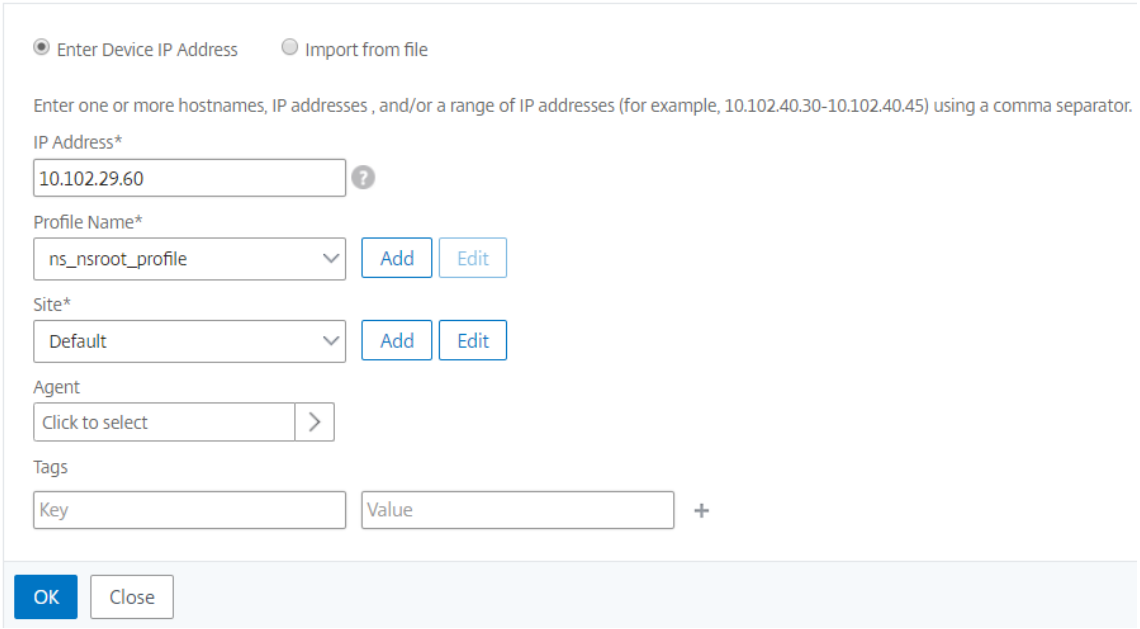
1. 导航到基础结构 **>** 实例 **> NetScaler**。在“实例”下，选择要添加的实例类型（例如 NetScaler VPX），然后单击“添加”。
2. 选择以下选项之一：

- 输入设备 **IP** 地址 -对于 NetScaler 实例，请指定每个实例的主机名或 IP 地址，或一系列 IP 地址。

- **Import from file**（从文件导入）- 上载包含要添加的所有实例的 IP 地址的文本文件。

3. （可选）选择首次登录失败时启用设备添加。使用此选项，即使没有有效凭据，您也可以添加实例。
4. 从 配置文件 名称中，选择适当的实例配置文件，或通过单击 **+** 图标创建配置文件。
5. 在 站点中，选择要添加实例的站点。
6. 在 代理中，选择要与实例关联的代理，然后单击 确定。

   如果您的 NetScaler 控制台上只配置了一个代理，则默认情况下会选择该代理。



在 **NetScaler** 控制台中添加 **NetScaler CPX** 实例

1. 导航到 **Infrastructure**（基础结构）**> Instances**（实例）。在“实例”下，选择 **NetScaler** 并选择 CPX 选项卡。
2. 单击添加。
3. 选择以下选项之一：

   - 输入设备 **IP** 地址。指定每个实例的主机名或 IP 地址，或 IP 地址范围。
   - 从文件导入。从您的本地系统上载包含要添加的所有实例 IP 地址的文本文件。

4. （可选）选择首次登录失败时启用设备添加。使用此选项，即使没有有效凭据，您也可以添加实例。
5. 在可路由 **IP/Docker IP** 字段中，输入 IP 地址。IP 地址可以是 NetScaler CPX 实例（如果可以访问的话）或 Docker 主机。
6. 在配置文件名称字段中，选择相应的实例配置文件，或单击 + 图标创建配置文件。

> 注意
>
> 创建配置文件时，请确保指定主机的 HTTP、HTTPS、SSH 和 SNMP 端口详细信息。您还可以在“起始端口”和“端口数”字段中指定主机发布的端口范围。

7. 作为选项，选择要部署 CPX 实例的站点。您也可以通过单击“添加”来创建站点。
8. 如果可用，请从代理列表中选择代理。
9. 单击“** 确定”启动向 NetScaler 控制台添加实例的过程。

> 注意
>
> ：如果要重新发现实例，请执行以下步骤：
>
> a) 导航到 基础结构 **>** 实例 **> NetScaler** > **CPX**。
> b) 选择要重新发现的实例。
> c) 在“选择操作”列表中，单击“重新发现”。

在 **NetScaler** 控制台中添加独立的 **NetScaler BLX** 实例

独立的 NetScaler BLX 实例是在专用主机 Linux 服务器上运行的单个实例。

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 在 **BLX** 选项卡中，单击 添加。
3. （可选）选择首次登录失败时启用设备添加。使用此选项，即使没有有效凭据，您也可以添加实例。
4. 从“实例类型”列表中选择“独立”选项。
5. 在 **IP** 地址 字段中，指定 BLX 实例的 IP 地址。
6. 在 主机 **IP** 地址 字段中，指定托管 BLX 实例的 Linux 服务器的 IP 地址。
7. 在 配置文件名称 列表中，为 BLX 实例选择相应的配置文件或创建配置文件。

   要创建配置文件，请单击“添加”。

   > 重要
   >
   > ：确保在配置文件中指定了 Linux 服务器的正确主机用户名和密码。

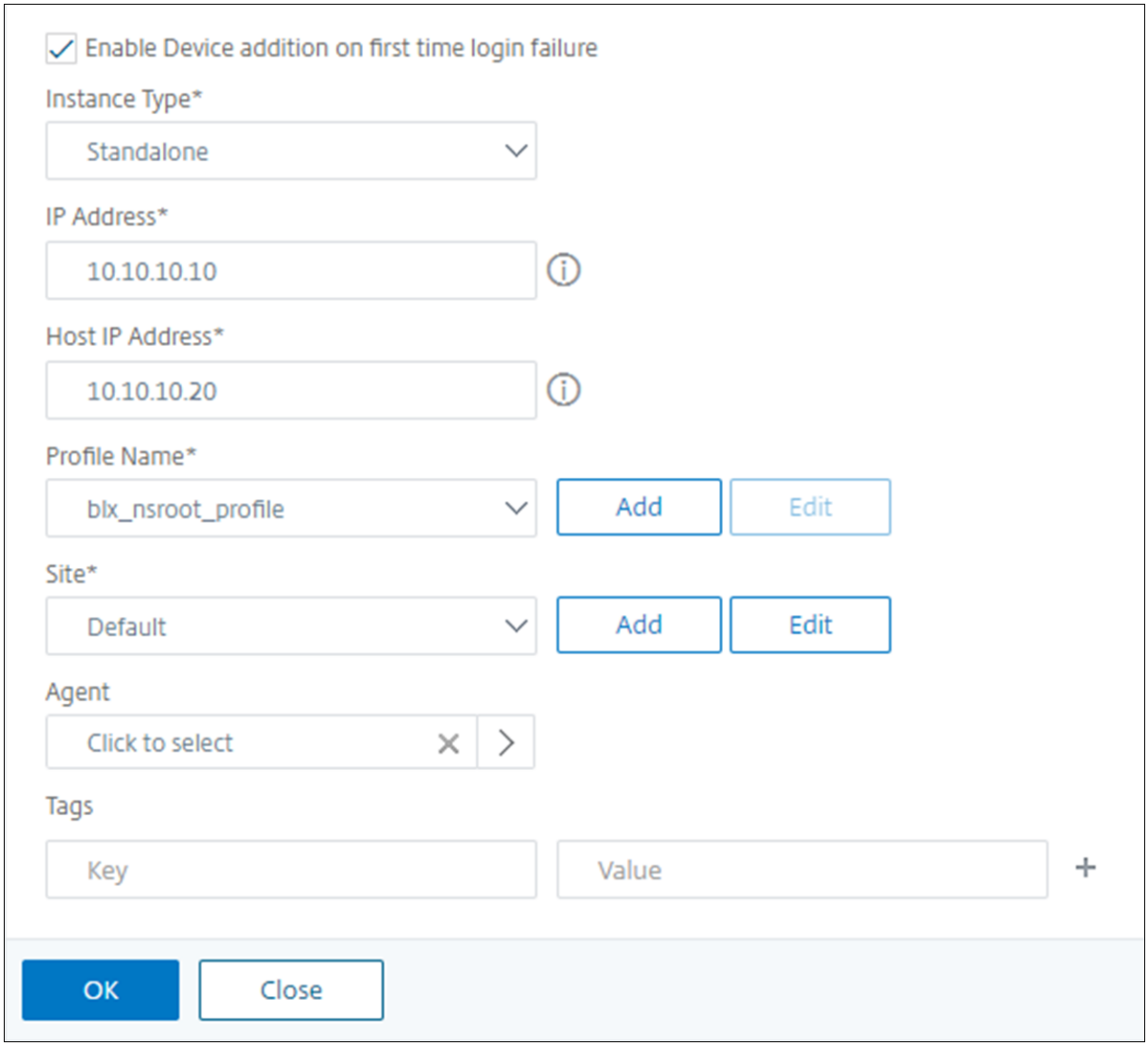
8. 在 站点 列表中，选择要添加实例的站点。

   如果要添加站点，请单击“添加”。

9. 在 代理列表中，选择要与该实例关联的代理。

   如果您的 NetScaler 控制台上只配置了一个代理，则默认情况下会选择该代理。

10. 单击确定。



在 **NetScaler** 控制台中添加高可用性的 **NetScaler BLX** 实例

在不同主机 Linux 服务器上运行的高可用性 NetScaler BLX 实例。一台 Linux 服务器不能托管多个 BLX 实例。

1. 在 **BLX** 选项卡中，单击 添加。
2. （可选）选择首次登录失败时启用设备添加。使用此选项，即使没有有效凭据，您也可以添加实例。
3. 从“实例类型”列表中选择“高可用性”选项。
4. 在 **IP** 地址 字段中，指定 BLX 实例的 IP 地址。
5. 在 主机 **IP** 地址 字段中，指定托管 BLX 实例的 Linux 服务器的 IP 地址。
6. 在“对 等 **IP** 地址”字段中，指定对等 BLX 实例的 IP 地址。
7. 在“对 等主机 **IP** 地址”字段中，指定托管对等 BLX 实例的 Linux 服务器的 IP 地址。

8. 在 配置文件名称 列表中，为 BLX 实例选择相应的配置文件或创建配置文件。

   要创建配置文件，请单击“添加”。

   > 重要
   >
   > ：确保在配置文件中指定了 Linux 服务器的正确主机用户名和密码。

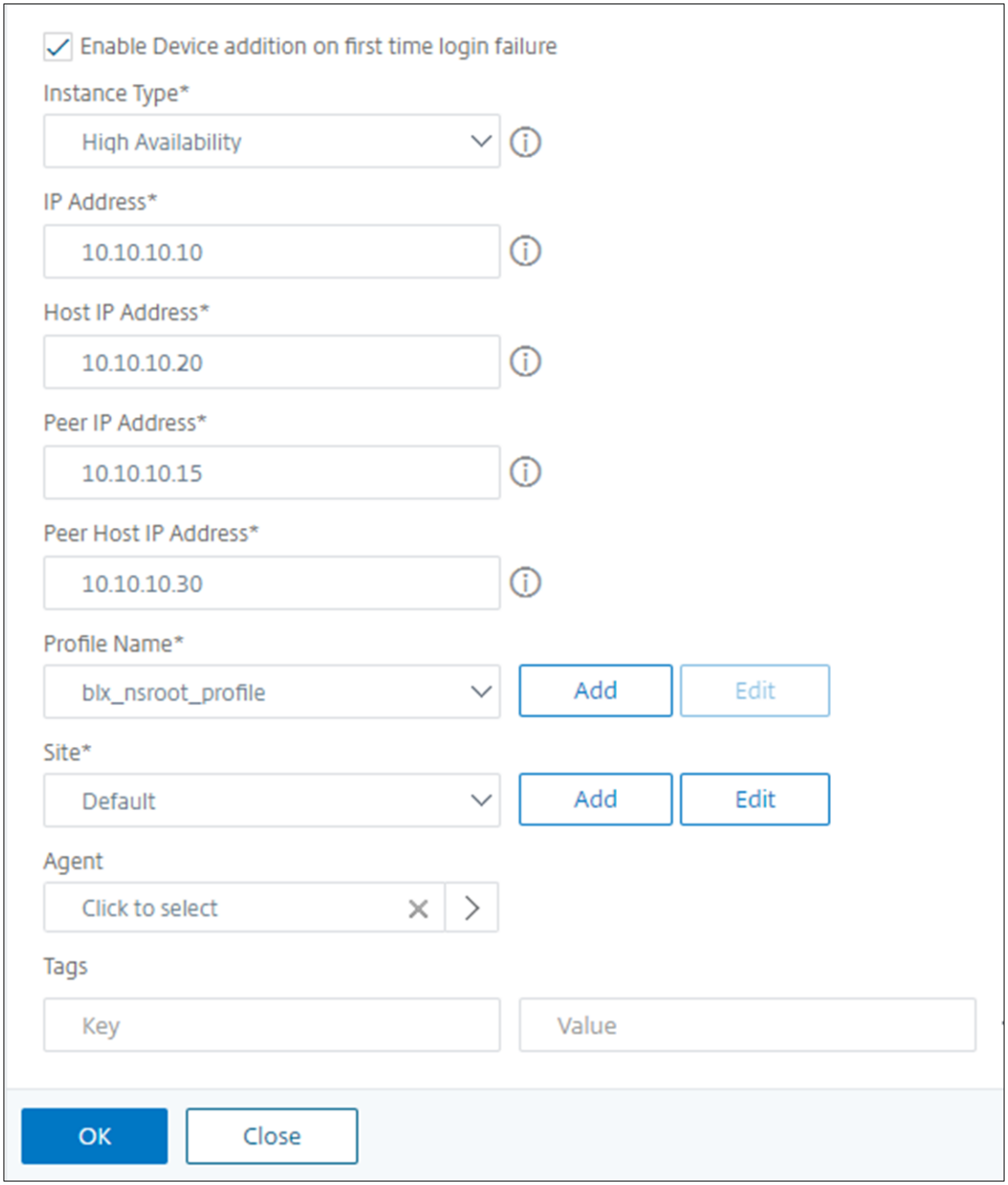
9. 在 站点 列表中，选择要添加实例的站点。

   如果要添加站点，请单击“添加”。

10. 在 代理列表中，选择要与该实例关联的代理。

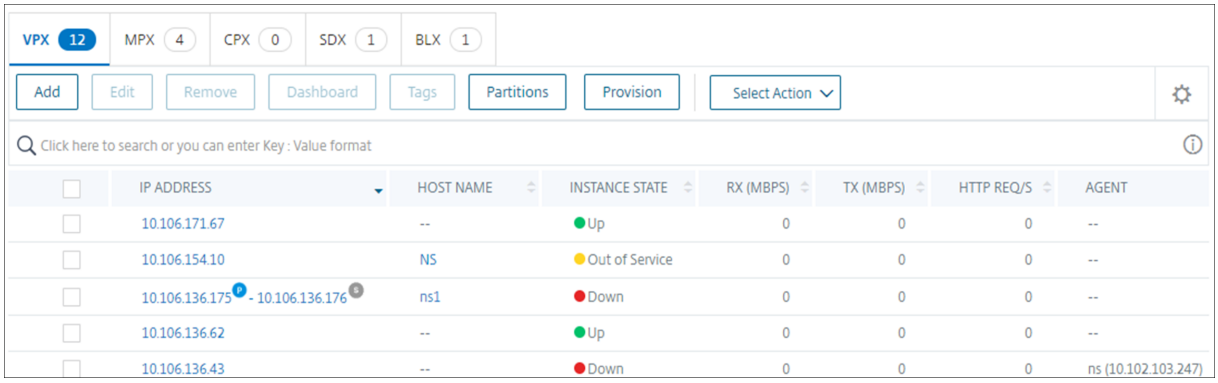
    如果您的 NetScaler 控制台上只配置了一个代理，则默认情况下会选择该代理。

11. 单击确定。



从 **NetScaler** 控制台访问实例 **GUI**

1. 导航到 基础架构 **>** 实例 **NetScaler**。
2. 选择要访问的实例类型（例如，VPX、MPX、CPX、SDX 或 BLX）。
3. 单击所需的 NetScaler IP 地址或主机名。



实例 IP 地址使用以下符号表示部署类型：

- 在高可用性对中，**P** -主服务器，**S** -辅助服务器。
- **C**-群集
- **A**-AutoScale 组

如果实例没有注解，则表示独立部署。

选定实例的 GUI 将显示在弹出窗口中。

解决实例警告

实例上会出现警告标志，原因如下：

- 登录失败 -当您添加没有有效凭据的实例时，该实例将处于关闭状态，并显示登录失败警告。在 NetScaler 控制台中指定用于管理实例的正确凭据。

  如果实例未获 许可，则当您选择实例时，将显示许可证选项。单击 许可证 将许可证应用于许可证池中的实例。
- 带有 **HTTPS** 配置文件的未许可实例 -如果未经许可的实例仅使用 HTTPS 连接，请从 NetScaler GUI 向实例申请许可。

在实例上配置 **syslog**

July 17, 2024

系统日志协议提供传输功能，允许 NetScaler 实例向 NetScaler 控制台发送事件通知消息，NetScaler 控制台被配置为这些消息的收集器或系统日志服务器。

如果您已将设备配置为将所有系统日志消息重定向到 NetScaler 控制台，则可以监视在 NetScaler 实例上生成的系统日志事件。要监视系统日志事件，首先需要将 NetScaler 控制台配置为 NetScaler 实例的系统日志服务器。配置实例后，所有系统日志消息都将重定向到 NetScaler 控制台，这样就可以以结构化的方式向用户显示这些日志。

Syslog 使用用户数据报协议 (UDP) 端口 514 进行通信，由于 UDP 是无连接协议，因此不向实例提供任何确认。syslog 数据包大小限制为 1024 字节并携带以下信息：

- 设施
- 严重性
- 主机名
- 时间戳
- 消息

在 NetScaler 控制台中，必须配置实例的设施和日志严重性级别。

- 设施 -Syslog 消息根据生成消息的来源进行大致分类。这些源可以是操作系统、进程或应用程序。这些类别称为设施，由整数表示。例如，0 用于内核消息，1 用于用户级消息，2 用于邮件系统，依此类推。本地使用设施（从 local0 到 local7）不是预留的，可供一般使用。因此，没有预先分配设施值的流程和应用程序可以定向到八个本地使用设施中的任何一个。
- 严重性 -生成 syslog 消息的来源或设施还使用个位数整数指定消息的严重性，如下所示：

```
1 - Emergency: System is unusable.

2 - Alert: Action must be taken immediately.

3 - Critical: Critical conditions.

4 - Error: Error conditions.

5 - Warning: Warning conditions.

6 - Notice: Normal but significant condition.

7 - Informational: Informational messages.

8 - Debug: Debug-level messages.
```

要在 **NetScaler** 实例上配置系统日志，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例。
2. 选择要从中收集系统日志消息并在 NetScaler 控制台中显示的 NetScaler 实例。
3. 在“操作”下拉列表中，选择“配置 **Syslog**”。
4. Click **Enable**。
5. 在 **Facility**（设施）下拉列表中，选择本地或用户级别的设施。
6. 为 syslog 消息选择所需的日志级别。
7. 单击确定。

这将配置 NetScaler 实例中的所有系统日志命令，然后 NetScaler 控制台开始接收系统日志消息。您可以通过导航到 **Infrastructure**（基础结构）**> Events**（事件）**> Syslog Messages**（**syslog** 消息）来查看消息。

Logstream 概述

March 10, 2024

NetScaler 实例生成 AppFlow 记录，是数据中心所有应用程序流量的中心控制点。**IPFIX** 和 **Logstream** 是将这些 AppFlow 记录从 NetScaler 实例传输到 NetScaler 控制台的协议。有关详细信息，请参阅 AppFlow。

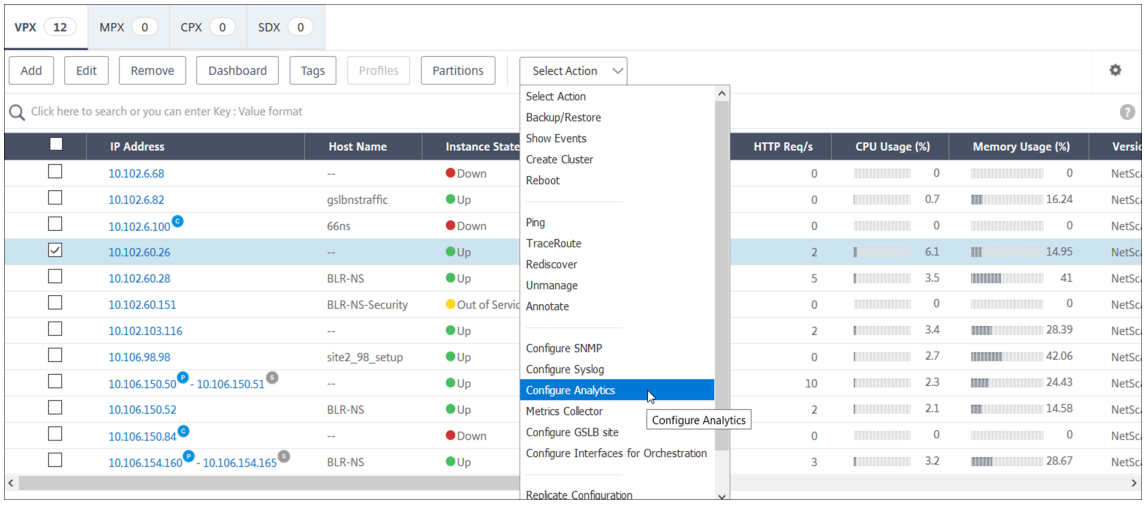
- **IPFIX** 是 RFC 5101 中定义的开放式 Internet 工程任务组 (IETF) 标准。**IPFIX** 使用 UDP 协议，这是一种不可靠的传输协议，用于单向数据流。由于 IPFIX 使用 UDP 协议，因此遵守 IPFIX 标准会在 NetScaler 控制台中处理更多资源。
- **Logstream** 是 Citrix 拥有的协议，用作传输模式之一，用于高效地将分析日志数据从 NetScaler 实例传输到 NetScaler 控制台。**Logstream** 使用可靠的 TCP 协议，处理数据所需的资源较少。

对于 **11.1 Build 47.14** 与 **11.1 Build 62.8** 之间的 NetScaler，**Logstream** 是启用 Web Insight (HTTP) 的默认传输模式，IPFIX 是启用其他见解的唯一传输模式。对于从 **12.0** 开始到最新版本的 NetScaler 版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

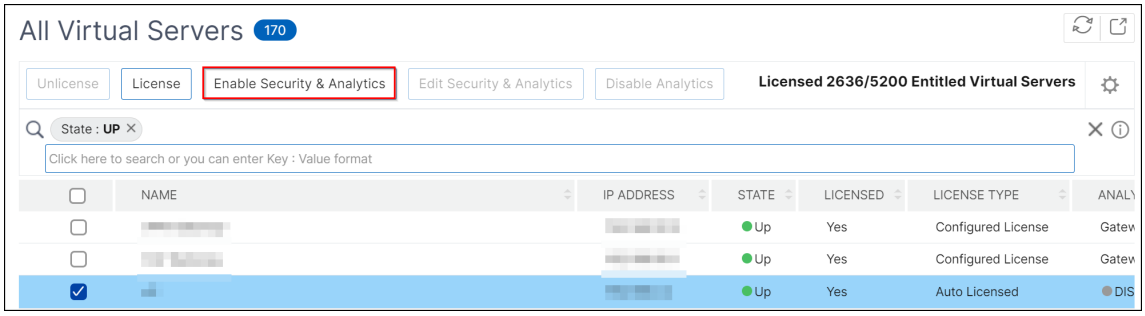
> 注意
>
> NetScaler 控制台版本和内部版本 必须等于或 高于您的 NetScaler 版本和内部版本。例如，如果您安装了 NetScaler 12.1 版本 50.28/50.31，请确保您已安装 NetScaler 控制台 12.1 版本 50.39 或更高版本。

启用 Logstream 作为传输模式

1. 导航到基础架构 **>** 实例，然后选择要启用分析的 NetScaler 实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。



3. 选择虚拟服务器，然后单击“启用安全和分析”。



4. 在“启用安全与分析”窗口中：

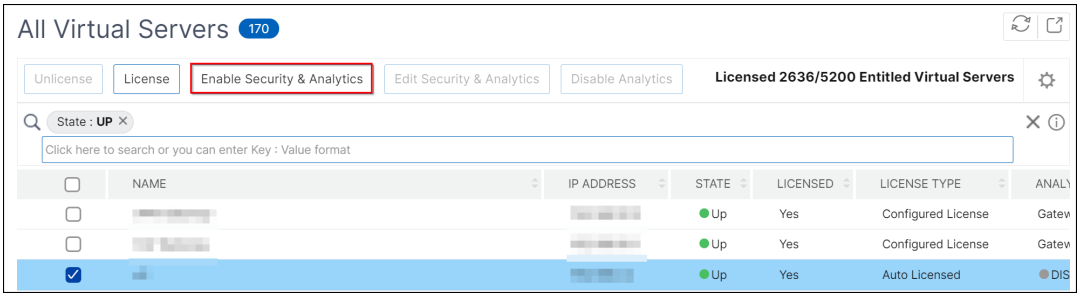
   a) 选择洞察类型（Web Insight 或 WAF 安全违规或 Bot 安全违规）

   b) 选择 **Logstream** 作为传输模式

   > 注意
   >
   > 对于 **11.1 Build 47.14** 与 **11.1 Build 62.8** 之间的 NetScaler，**Logstream** 是启用 Web Insight (HTTP) 的默认传输模式，IPFIX 是启用其他见解的唯一传输模式。对于从 **12.0** 开始到最新版本的 NetScaler 版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。

   c) 默认情况下，表达式为 true

   d) 单击保存分析



> 注意
>
> - 对于管理分区，仅支持 **Web Insight**
> - 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。将显示一条错误消息。

下表描述了支持 **Logstream** 作为传输模式的 NetScaler 控制台的功能：

功能	**IPFIX**	**Logstream**
Web Insight	•	•
机器人安全违规	不支持	•
WAF 安全违规	•	•

功能	IPFIX	Logstream
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

如何向委派管理员用户分配更多权限

January 29, 2024

当您组织的第一个用户注册并登录 NetScaler 控制台时，该用户将被分配超级管理员权限。默认情况下，每个后续登录的用户都会被分配一个委托的管理员角色。委派管理员无权查看和执行与用户管理或 RBAC 设置相关的任何任务。

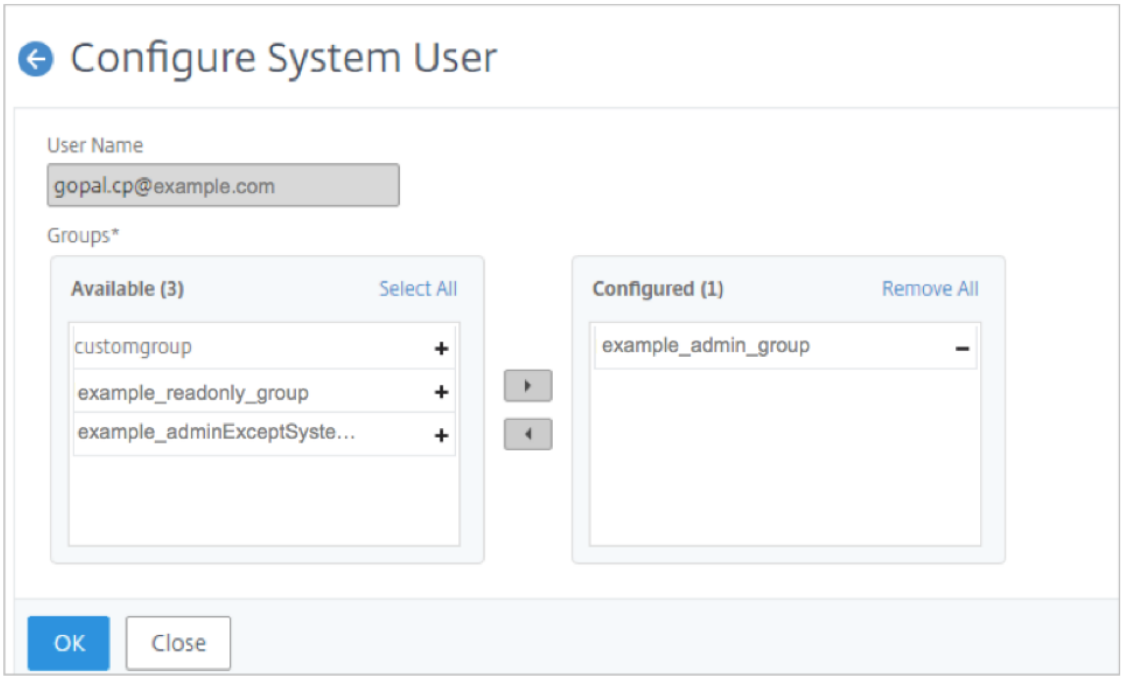
但是，您可以将超级管理员权限或特定的非超级管理员角色分配给委派管理员，以便管理员能够执行与用户管理相关的任务。

有关基于角色的访问控制的详细信息，请参阅 配置基于角色的访问控制。

向委派管理员分配超级管理员权限

要向委派的管理员分配超级管理员权限，超级管理员必须将默认管理员组分配给委派的管理员用户。请执行以下任务：

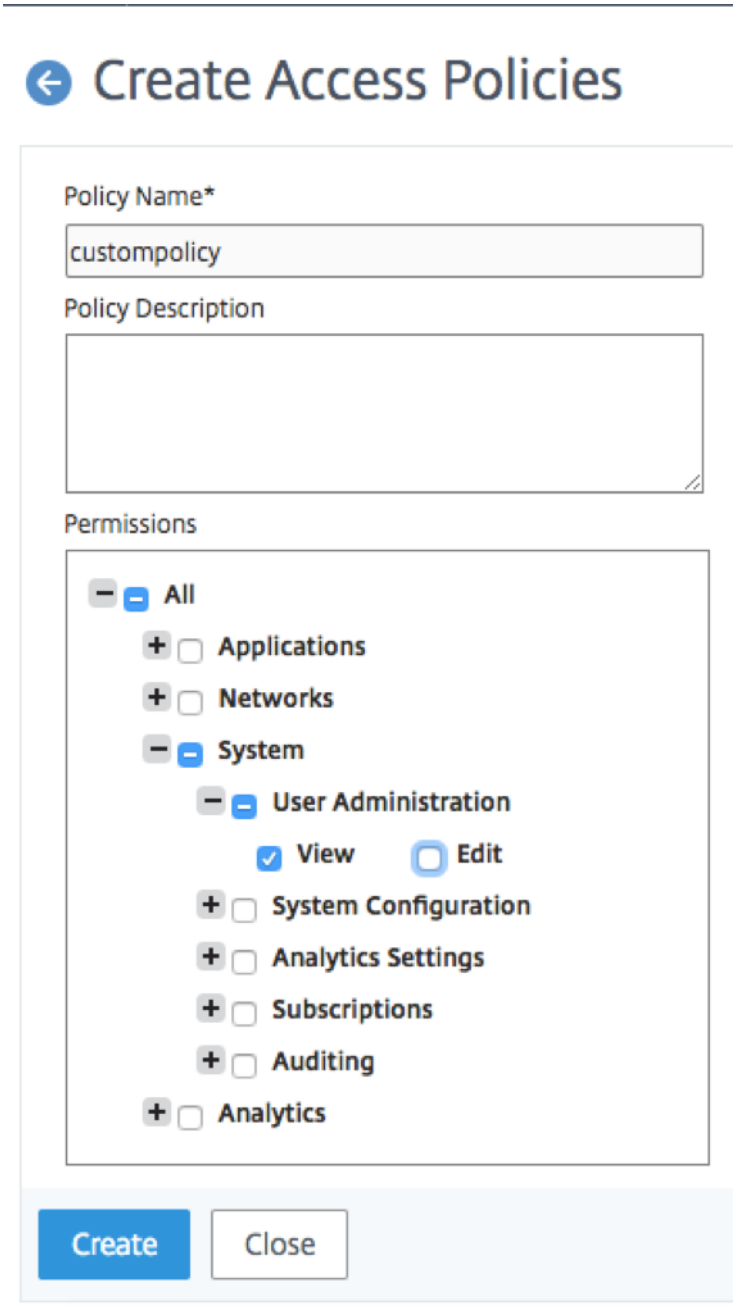
1. 以超级管理员身份登录 NetScaler 控制台。
2. 导航到“帐户”>“用户管理”>“用户”。
3. 选择委派管理员的用户名，然后单击“编辑”。
4. 将组 **<** 租户名称 **>_admin_group** 分配给委派的管理员，然后单击确定。例如，在下图中，“example_admin_group”被分配给委派管理员用户。



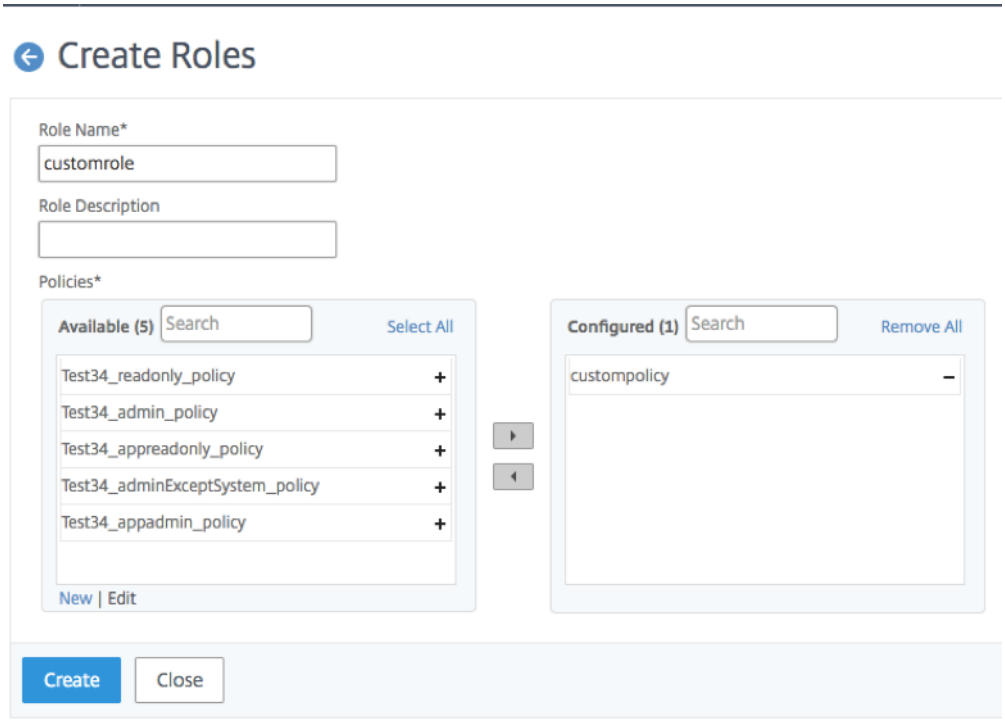
将自定义角色分配给委派管理员

要将任何自定义角色分配给委派管理员，超级管理员必须创建组、角色和策略，然后将其分配给委派的管理员用户。这可确保委派管理员只具有所需的权限。请执行以下任务：

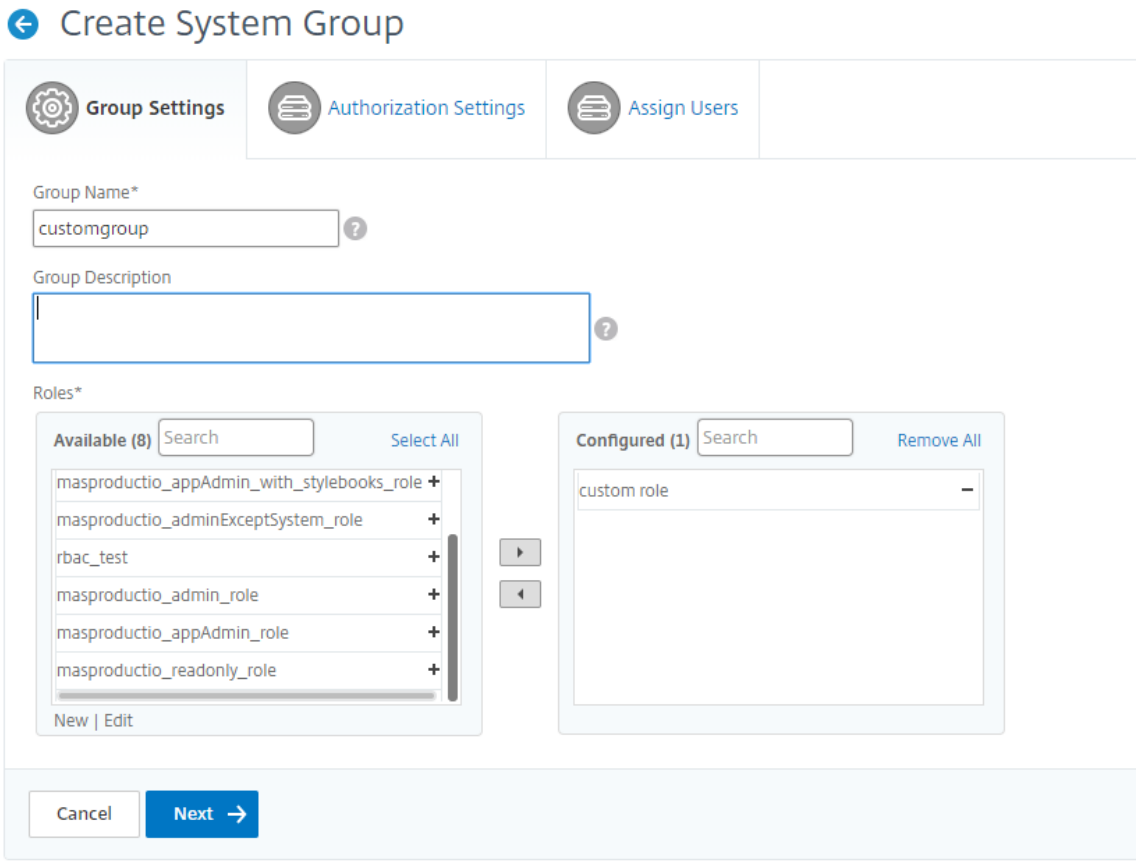
1. 以超级管理员身份登录 NetScaler 控制台。
2. 导航到“帐户”>“用户管理”>“访问策略”。选择 添加 以创建具有委派管理员所需权限的访问策略。在此示例中，创建了允许查看访问用户管理设置的访问策略 `custompolicy`。



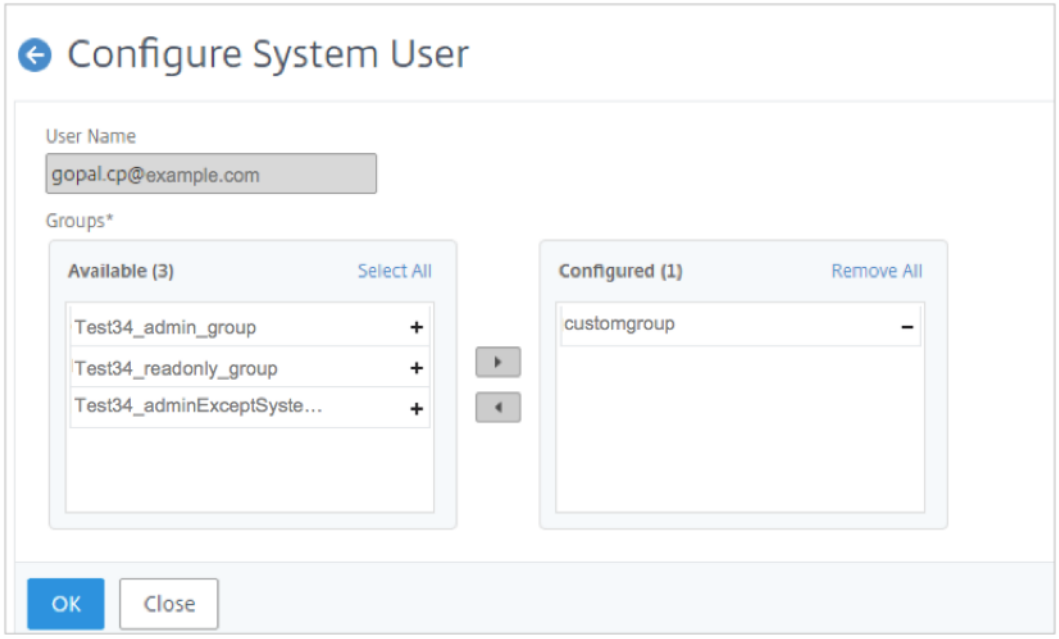
3. 导航至 帐户” > “用户管理 > 角色。选择添加 以创建角色，并将此角色绑定到您在上一步中创建的访问策略。在此示例中，创建了角色 `customrole` 并将其绑定到 `custompolicy` 访问策略。



4. 导航至 帐户” > “用户管理 > 组。选择添加 以创建组，并将此组绑定到您在上一步中创建的角色。在此示例中，创建组“自定义组”并绑定到角色“自定义角色”。



5. 导航到 帐户 **>** 用户管理 > 用户
6. 选择委派管理员的用户名，然后单击“编辑”。
7. 将您在上一步中创建的组分配给委派的管理员用户。在此示例中，已向委派管理员用户分配了组 `customgroup`。



与 **ServiceNow** 实例集成

April 10, 2024

作为 NetScaler 管理员，您可以使用 ServiceNow 作为主要的 IT 请求和支持系统。您需要为关键 NetScaler 事件举报单或事件，以进行调查、跟踪和故障排除。

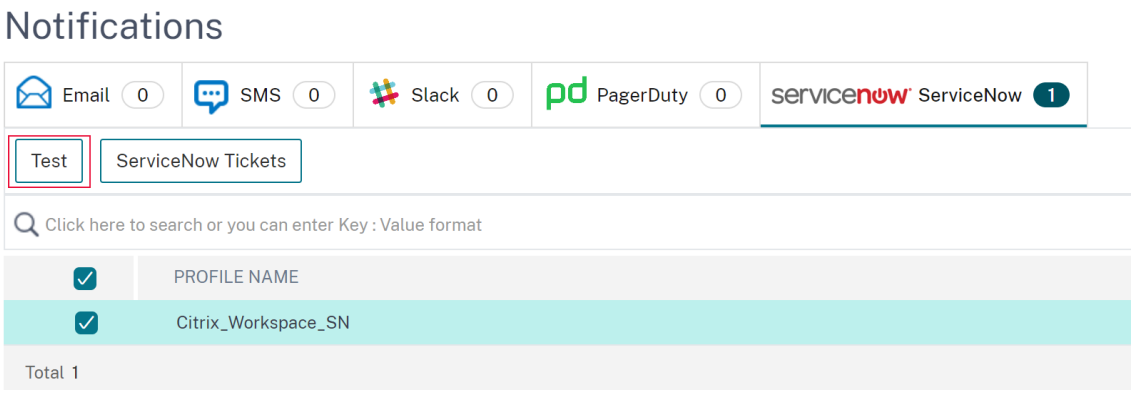
您可以使用 NetScaler 控制台和适用于 ServiceNow 的 Citrix ITSM Connector 在 ServiceNow 中自动创建票证。要启动这种自动化，请加载 Citrix ITSM 适配器服务以接收事件并在 ServiceNow 中创建相关事件。有关准备和集成步骤的更多信息，请参阅 Citrix ITSM 适配器服务中的入门。

成功集成后，在 NetScaler 控制台中配置自动生成 ServiceNow 事件。按照以下步骤验证 ServiceNow 票证是否自动生成。

1. 登录 NetScaler 控制台。
2. 导航到“设置” **>** “通知”，然后选择 **ServiceNow**。
3. 从列表中选择 ServiceNow 配置文件。

4. 单击“测试”自动生成 ServiceNow 票证并验证配置。

   如果您想在 NetScaler 控制台 GUI 中查看 ServiceNow 票证，请选择 **ServiceNow** 票证。



当您将 NetScaler 控制台与 ServiceNow 集成时，您可以针对以下情况自动生成 ServiceNow 事件：

- 任何 NetScaler 事件
- 即将到期的 SSL 证书
- NetScaler 控制台许可到期事件

而且，您还可以自定义 NetScaler 控制台事件策略。

为任何 **NetScaler** 事件生成 **ServiceNow** 事件

在 NetScaler 控制台中，您可以配置规则，自动在 ServiceNow 中为特定事件出票。NetScaler 控制台会自动为以下事件生成 ServiceNow 票证：

- 虚拟服务器停机或停止服务。
- 资源消耗超过阈值。
- NetScaler 实例的许可到期。

ServiceNow 中自动生成的票证包含跟踪和解决问题所需的详细信息。您可以通过单个 ServiceNow 控制台管理一台或多台网络设备上的通知。然后，分配给管理员进行进一步分析。

您可以导航到 基础架构 > 事件 > 规则，在 **NetScaler** 控制台上创建事件规则。有关详细信息，请参阅 发送 ServiceNow 通知。

为即将到期的 **SSL** 证书生成 **ServiceNow** 事件

当 NetScaler 实例上的 SSL 证书即将到期时，NetScaler 控制台会自动生成 ServiceNow 票证。这样，您就可以在 SServiceNow 控制面板上提前查看即将到来的 SSL 证书到期凭据。

要发送 SSL 证书到期的 ServiceNow 通知，请参阅 SSL 证书到期。

为 **NetScaler** 控制台许可到期生成 **ServiceNow** 事件

在 NetScaler 控制台中，您可以将规则配置为在 ServiceNow 中针对特定的 NetScaler 控制台许可到期事件自动出票。

要发送 NetScaler 控制台许可到期的 ServiceNow 通知，请参见 NetScaler 控制台许可到期。

自定义 **NetScaler** 控制台事件策略

您可以定义策略，控制 ServiceNow 如何根据事件属性处理 NetScaler 控制台事件。在 Citrix ITSM 连接器中设置 NetScaler 控制台事件策略。您可以决定如何在 ADM 中生成、处理和报告事件。然后，通过 ITSM 执行以下操作：

- 忽略事件
- 在控制板上显示事件
- 创建事件

有关更多信息，请参见 自定义 NetScaler 控制台事件策略。

可操作的任务和建议

June 7, 2024

> 注意：
>
> - 待办事项选项卡已重命名为“建议”。在“建议”中，您可以继续查看现有任务，然后单击“引导我”以完成任务。
> - “存档”选项卡不再可用。相反，您可以选择消除列表中的建议。

您可能发现了数百个 NetScaler 实例，并从每个实例配置了多个虚拟服务器（应用程序）。作为管理员，您必须确保有效管理所有 NetScaler 实例和应用程序，以获得见解，从而更好地确定优先级和进行故障排除。

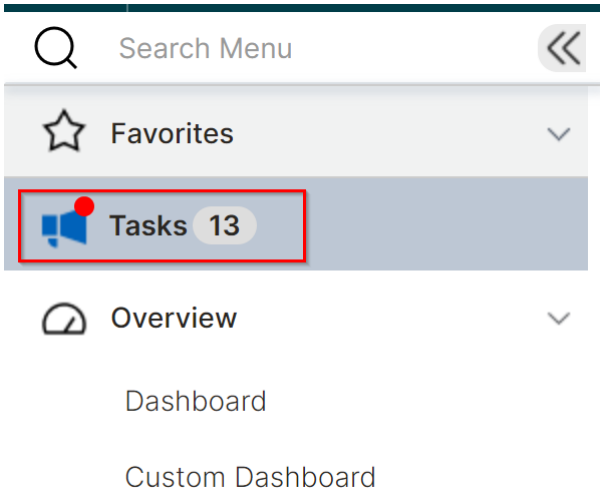
随着您进一步扩展基础架构，您可能还需要将注意力集中在影响实例和应用程序的关键问题上，这些问题需要立即关注。您还必须确保您的 NetScaler 控制台部署高效、安全且合规。根据您当前的使用情况和订阅情况，NetScaler 控制台中的任务 功能使您能够查看必须立即采取操作 的可操作 任务 和 确保高效部署的建议。

作为管理员，通过使用这些可操作的 任务 和 建议，您可以：

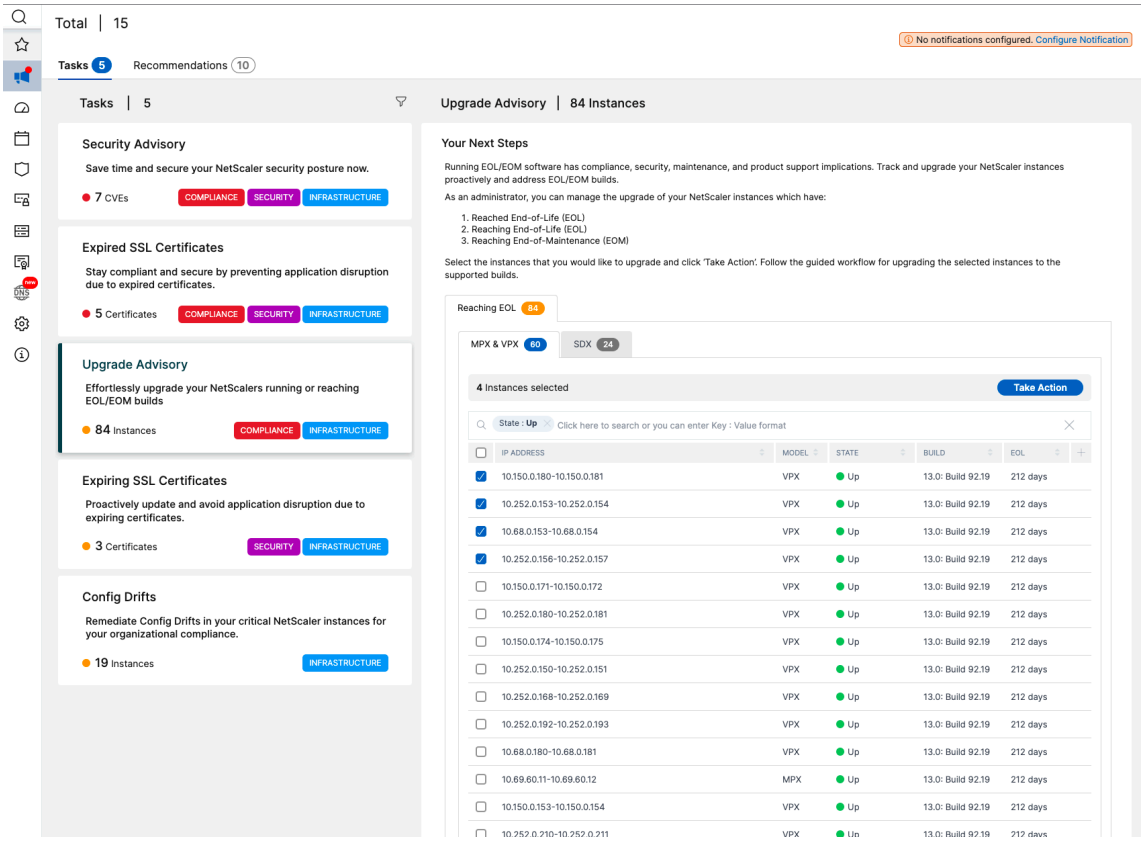
- 即时了解需要您立即采取操作的任何观察结果或问题。
- 将通知配置为在 NetScaler 控制台检测到任何任务时接收通知并主动采取措施。
- 实现 NetScaler 控制台和 NetScaler 实例的高效部署。
- 减少识别关键问题的关键时间和精力。

- 确保您充分利用 NetScaler 控制台的所有功能，启用产品发现和产品推荐的功能，以便高效管理部署。

在 NetScaler 控制台 GUI 中，单击“任务”以查看任务和建议。

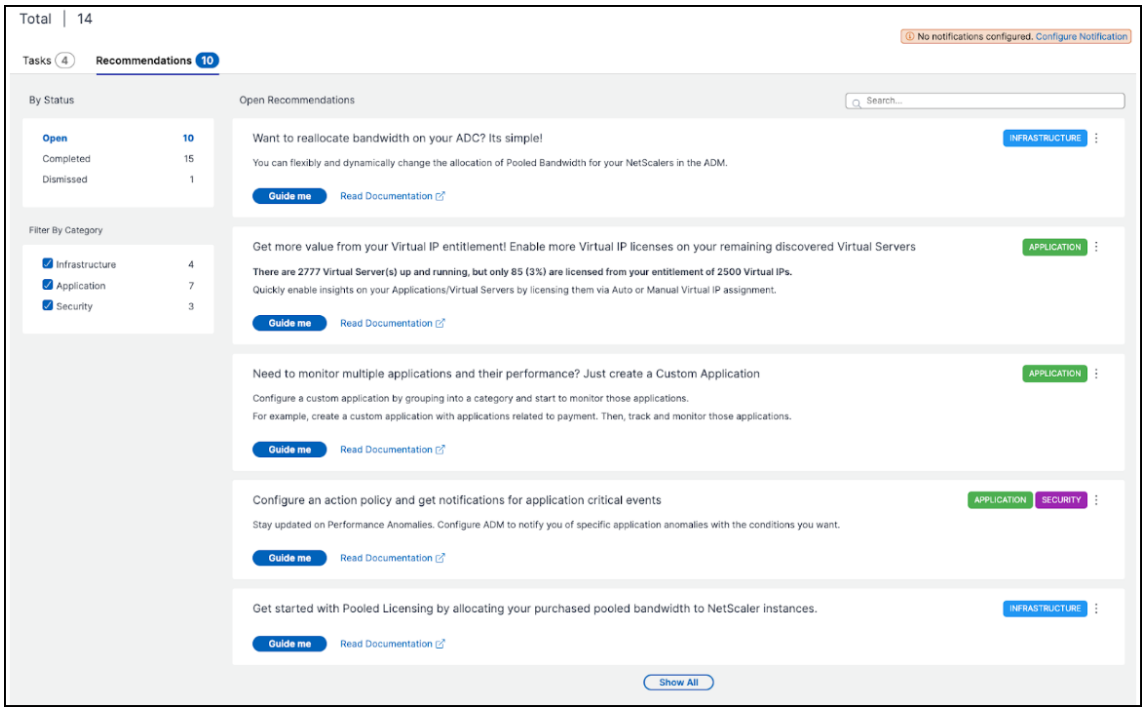


- 任务 -使您能够查看需要立即关注和操作的任务列表。当您扩展基础设施时，一些关键问题可能会被忽视，从而导致安全漏洞。例如，需要立即关注带有 CVE 的 NetScaler 实例，您必须立即采取措施确保实例以推荐的版本和版本运行。在 任务中，您可以立即获得这些见解。根据您当前的使用率，您总共可以查看 5 个任务。任务根据严重性（严重和中等）显示。



- 建议-根据您的当前使用情况提供某些建议，以改进 NetScaler 控制台的部署。您可以使用“指导我”选项来完成任何建议。您使用“指导我”选项完成的任何建议都将移至“已完成”。您也可以驳回任何建议，这些建议将移至“已 驳回”类别下。要查看已被驳回的建议，请使用 按状态 筛选并选择已 驳回 以查看那些被驳回的建议。

  您还可以使用 按类别筛选根据类别（基础架构、应用程序和安全）筛选特定的建议。或者，您也可以使用 搜索栏，键入前几个字符向下钻取任务。



任务

在“任务”下，您可以查看以下 4 个任务，具体取决于您当前 NetScaler 控制台的部署。

- **SSL** 证书已过期—提供有关安装在 NetScaler 控制台中的过期 SSL 证书的信息。选择此任务可查看以下选项卡：
  - 删除未使用的证书：显示未在任何 NetScaler 实例中使用的证书。要完成任务，请查看未使用的证书，选择证书，单击“查看并删除”。

    推荐操作：您将被重定向到基础结构 **> SSL** 控制板 **> SSL** 证书 **-** 已过期。要删除证书，请单击“删除”。如果要更新证书，请选择证书并单击“更新”。有关更多信息，请参阅如何更新已安装的证书。
  - 更新证书：显示已经过期的证书。要完成任务，请查看证书，选择证书，然后单击“查看和更新”。

    推荐操作：您将被重定向到基础结构 **> SSL** 控制板 **> SSL** 证书 **-** 已过期。选择证书，然后单击“更新”或“删除”。有关更多信息，请参阅如何更新已安装的证书。
- **SSL** 证书即将 过期-提供有关即将过期的 SSL 证书的信息。

建议的操作：选择此任务可根据到期日期前的总天数查看选项卡。要完成任务，请从选项卡中选择证书，然后单击“查看和更新”。您将被重定向到 基础架构 **>** **SSL** 控制面板中的相关页面。选择证书并单击“更新”。有关更多信息，请参阅如何更新已安装的证书。

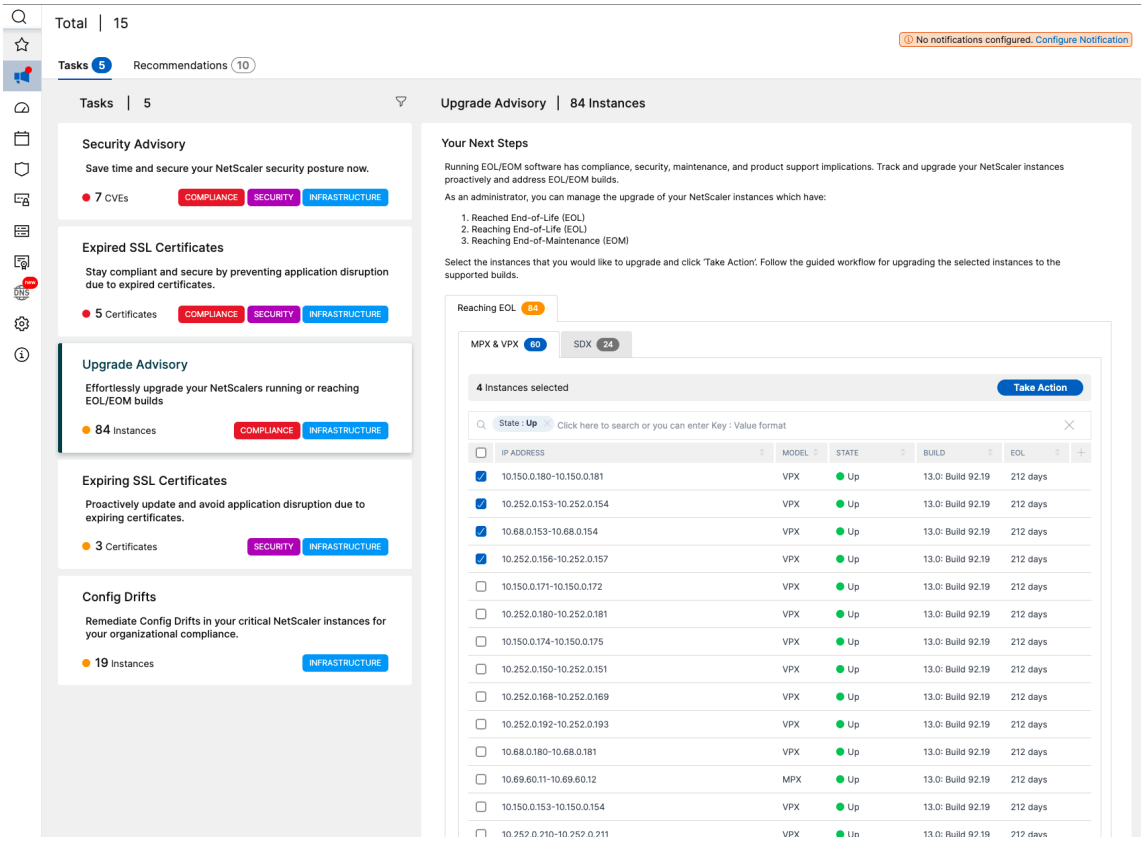
- **Config Drift** s —提供有关 NetScaler 实例中配置偏差（已保存与运行差异以及模板与运行差异）的信息。选择此任务可查看以下选项卡：
  - 配置未保存的实例：您可以查看具有未保存配置的实例。要完成任务，请选择实例，单击“查看并保存配置”。

    推荐操作：您将被重定向到 基础架构 **>** 配置 **>** 配置审核 **>** 审核报告，您可以查看具有未保存配置的实例。单击“保存配置”以完成此任务。有关更多信息，请参阅 文档。
  - 与模板存在偏差的实例：您可以查看存在模板偏差的实例。要完成任务，请选择实例，单击“查看并运行正确的命令”。

    建议的操作：您将被重定向到 基础架构 **>** 配置 **>** 配置审核 **>** 审核报告，您可以查看存在模板偏差的实例。按照文档完成任务。
- 安全公告 - 提供有关影响您的 NetScaler 实例的 CVE 的信息。选择此任务可查看以下选项卡：
  - 检测到的 **CVE**：显示检测到的 CVE 以及影响 CVE 的 NetScaler 实例。要完成此任务，请选择 CVE，单击“查看并修复”。

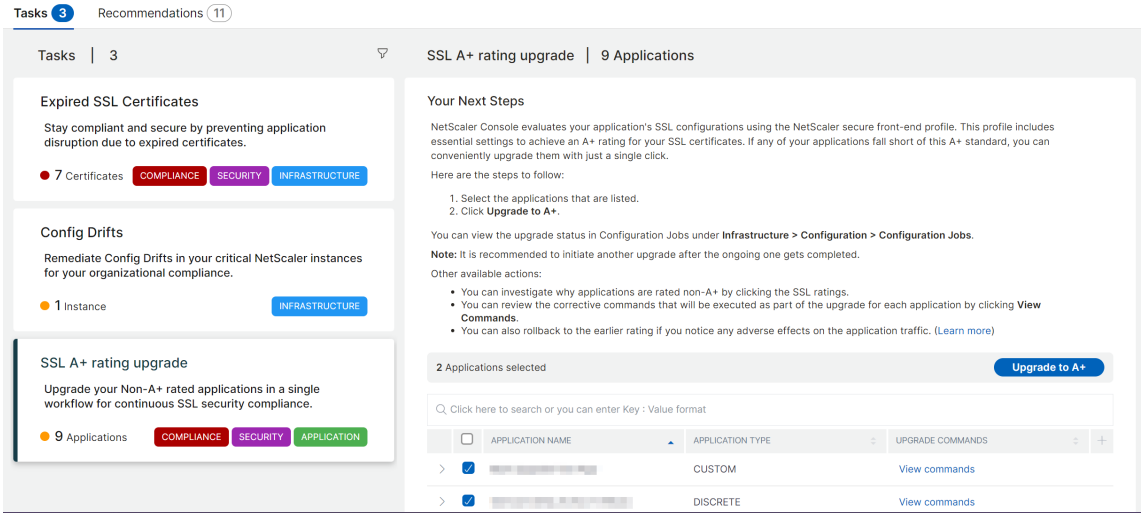
    推荐操作：您将被重定向到基础结构 **>** 实例公告 **>** 安全公告中的安全公告页面。按照文档完成任务。
  - 受影响的实例：显示受到 CVE 影响的 NetScaler 实例。要完成任务，请选择实例，单击“查看并修复”。

    推荐操作：您将被重定向到基础结构 **>** 实例公告 **>** 安全公告中的安全公告页面。按照文档完成任务。
- 升级建议：提供有关在 90 天内已经达到或即将达到生命周期终止 (EOL) 或维护终止 (EOM) 的 NetScaler 实例的信息。



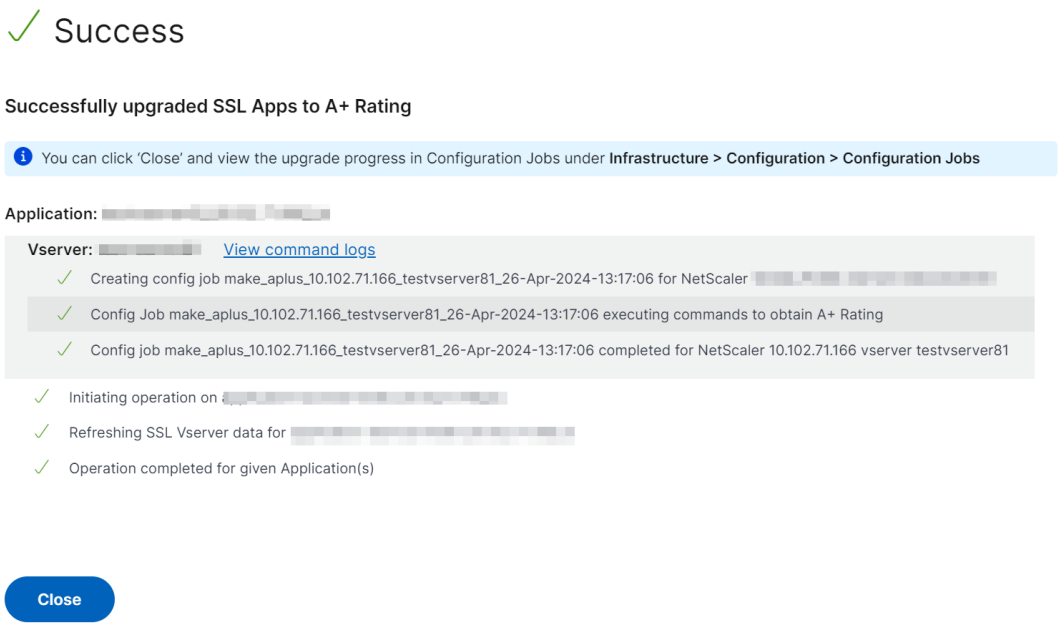
推荐的操作：单击“采取操作”，将实例升级到推荐的版本。

- **SSL A+** 评级升级：提供有关不符合 A+ 评级的应用程序的信息。



推荐的操作：从列表中选择应用程序，然后单击“升级到 **A+**”。

升级成功后，您可以看到以下成功消息：

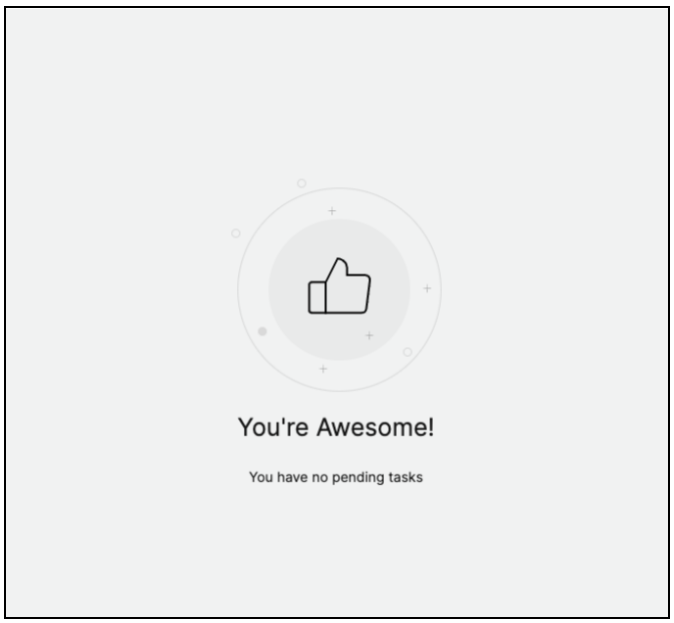


升级完成后，应用程序详细信息将从任务中删除。

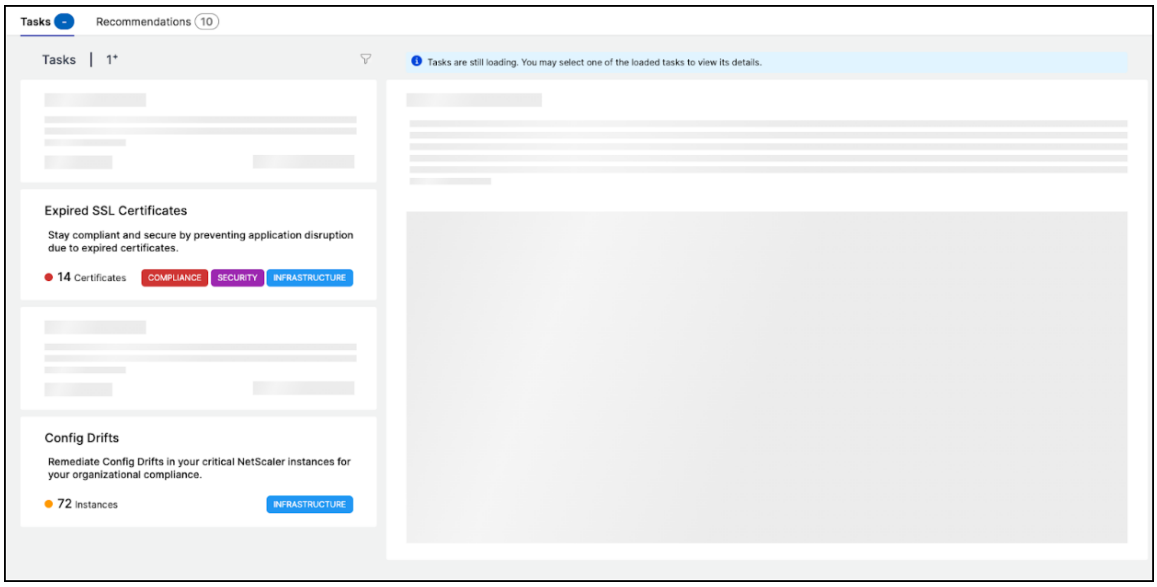
注意事项：

- 根据所选应用程序的数量，升级完成过程的持续时间可能会有所不同。
- 启动升级过程后，建议在正在进行的升级过程完成后启动另一个升级过程。
- 您还可以在基础架构 **>** 配置 **>** 配置作业中查看升级过程的状态。
- 如果升级过程不成功，则可以在基础架构 **>** 配置 **>** 配置作业中查看状态。您可以再次从任务启动升级过程。
- 如果您进行批量升级，并且一个或多个应用程序升级失败，则只能在任务中查看失败的应用程序的详细信息。您可以再次启动升级过程以完成升级。

> 注意：
>
> - 如果您的 NetScaler 控制台没有任何待处理任务，则可以查看以下页面：



- 在某些情况下，检查会在所有实例上进行，加载所有任务可能需要更多时间。



建议

下表描述了您可以在 NetScaler 控制台 GUI 中查看的建议：

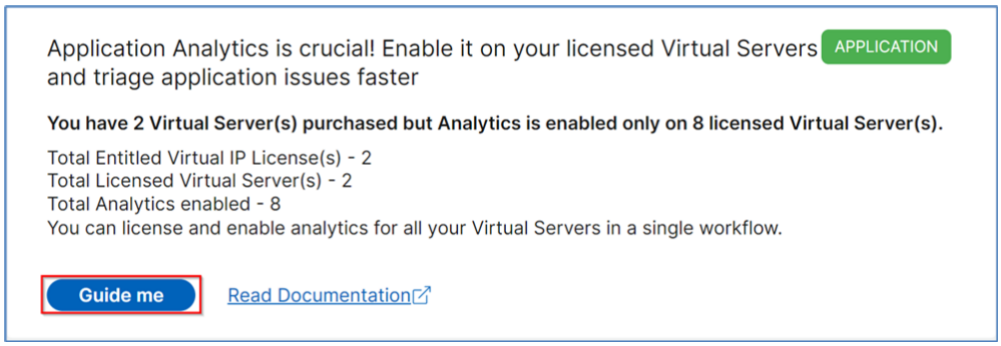
> 注意
>
> 对于合并许可，您可以根据现有的合并许可权获得建议。

建议名称	任务何时在 GUI 中可见?
添加 NetScaler 实例	在您加入 NetScaler 控制台之后，如果未发现任何 NetScaler 实例。
添加外部代理以充分利用 NetScaler 控制台中的最大功能	如果未配置外部代理。您可以开始使用内置代理。但是，外部代理需要使用所有功能，例如分析、池许可等。
将 NetScaler 从内置代理注册到外部代理	使用服务连接工作流程加载 NetScaler 控制台后，将使用内置代理加载 NetScaler 实例。您可以将这些 NetScaler 实例注册到外部代理，以使用分析、池化许可等所有功能。
应用程序分析至关重要！在许可的虚拟服务器上启用它，可以更快地对应用程序问题进行分类。	如果您有多个许可的虚拟服务器但未启用分析功能。
想在 NetScaler 上重新分配带宽吗？很简单！	如果在 NetScaler GUI 中分配了池化许可，并且在 NetScaler 控制台中发现了这些 NetScaler 实例，则可以使用 NetScaler 控制台进行重新分配。
从您的虚拟 IP 权利中获得更多价值！在发现的剩余虚拟服务器上启用更多虚拟 IP 许可证	如果您拥有所需的许可证，但未获得所有虚拟服务器的许可。
为您的关键企业用户启用基于精细角色的访问权限	如果尚未在 NetScaler 控制台中配置基于角色的访问控制 (RBAC)。
配置规则，永远不会错过 NetScaler 实例上的任何关键事件	如果尚未配置自定义事件规则。
需要监视多个应用程序及其性能吗？只需创建一个自定义应用程序	如果尚未配置自定义应用程序。
通知应用程序中的关键事件，切勿错过这些事件	如果未针对应用程序评分偏差、服务器处理时间、客户端网络延迟、服务器网络延迟或响应时间配置操作策略。
避免应用程序中断，也不要错过应用程序中即将过期的 SSL 证书	如果没有为即将到期的 SSL 证书配置警报或通知。
安全公告-利用 CVE 和缓解措施让您的 NetScaler 实例保持最新状态	NetScaler 实例是否有任何 CVE 影响。
配置企业策略并监视是否存在任何偏差	如果 SSL 企业设置未更改或仍处于默认状态。
手动重复任务？创建配置任务并将其应用于多个 NetScaler 实例	如果尚未配置作业任务。
通过选择您选择的自定义指标来管理和监视您的实例评分。	如果未修改实例评分设置中的默认设置和阈值。
通过选择您选择的自定义指标来跟踪您的应用程序评分	如果默认使用应用程序控制板中的“应用程序评分”组件且未进行自定义。
添加专用 IP 块以在地理地图中可视化客户端请求	如果未配置 IP 块。您可以创建 IP 块，根据其专用 IP/范围在地理地图上映射和可视化客户端请求。
订阅您的 AppSec 违规行为并将其实时导出到 Splunk	如果尚未配置 NetScaler 控制台中的 Splunk 集成。

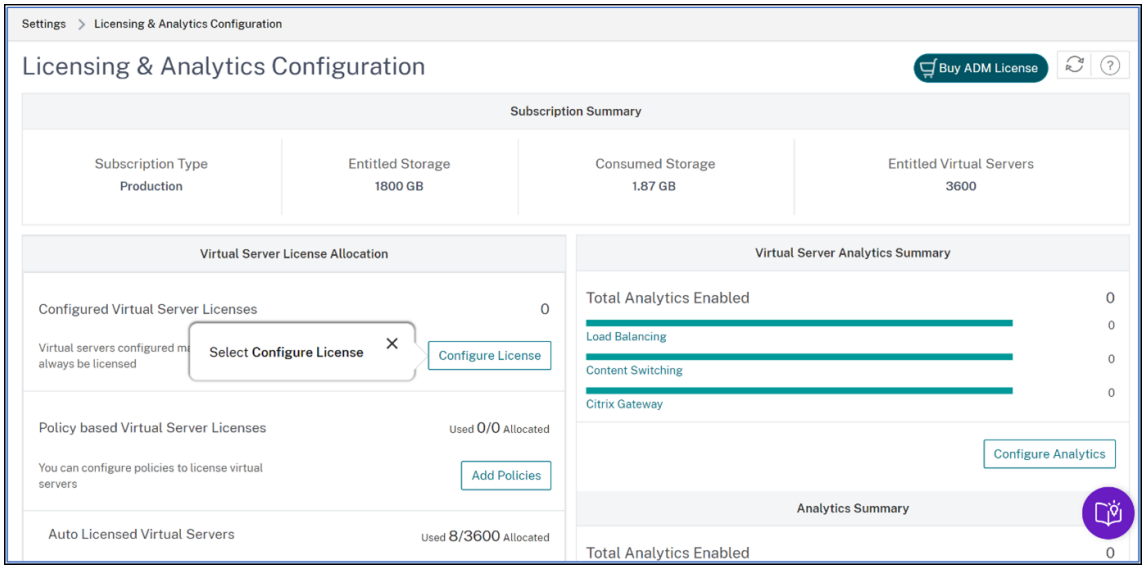
建议名称	任务何时在 GUI 中可见?
自定义默认阈值或为您的 Kubernetes 服务创建新的阈值	如果在服务图中仅使用默认阈值，并且不对服务应用任何单阈值或双阈值。
主动配置通知配置文件并在通信目的地接收通知	如果尚未配置通知配置文件。
安排定期导出并获取有关基础结构详细信息的通知	如果尚未在基础结构 **>** 实例中配置导出计划。
有 ServiceNow 并且想与 ADM 集成吗?	如果尚未配置 NetScaler 控制台中的 ServiceNow 集成。
使用 Venafi 和 ADM 自动管理 SSL 证书	如果尚未在 NetScaler 控制台中配置 Venafi 服务器。
在您的共用许可证到期之前续订它。	如果您的现有许可证将在 30 天后过期。
将购买的池化带宽分配给 NetScaler 实例，开始使用池化许可。	如果您尚未开始分配您的合并许可证权利。
考虑购买更多的共用带宽容量。	如果您已使用 90%或更多的共用带宽。
您当前的共用带宽权限未得到充分利用。审查并考虑分配更多资金	如果您的合并许可证分配利用率低于 70%。

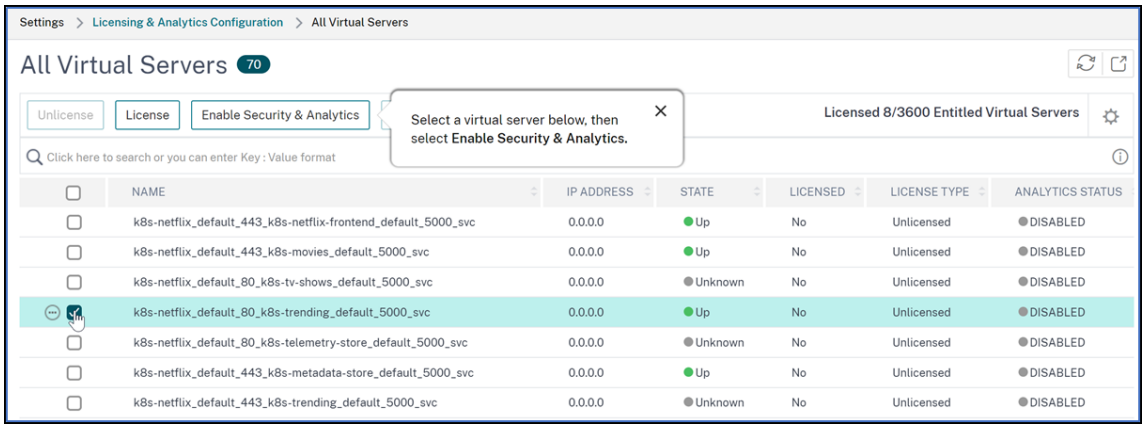
如何使用 **Guide me** 工作流程并完成推荐

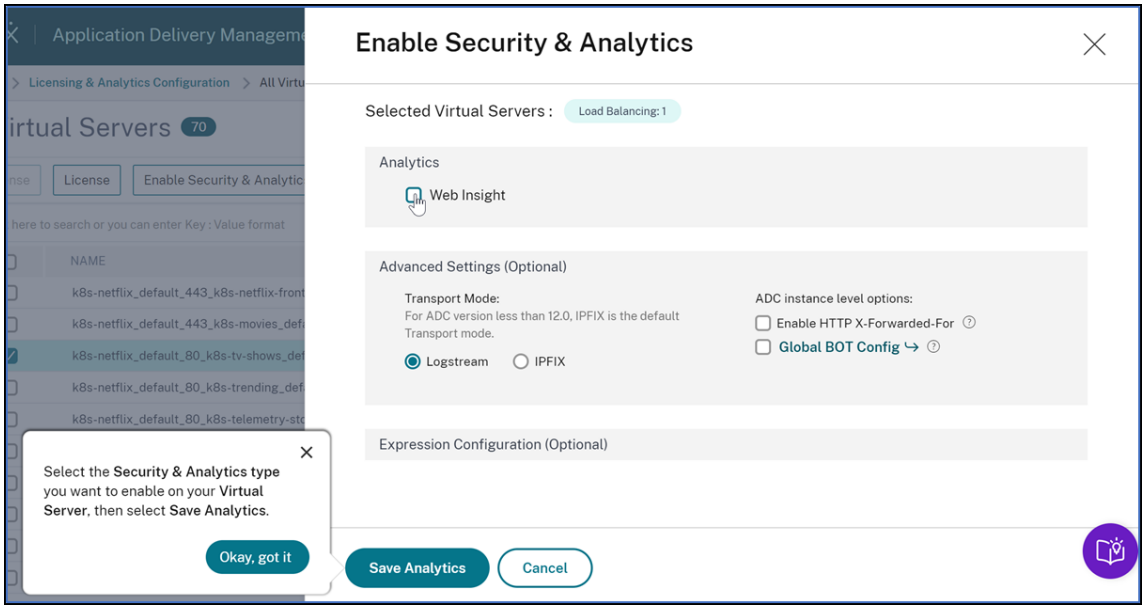
假设您要为所有虚拟服务器启用分析。单击“引导我”执行以下任务：



该工作流程提供了完成任务所需的建议。在此示例中，单击引导我后，按照提供的工具提示建议进行操作：

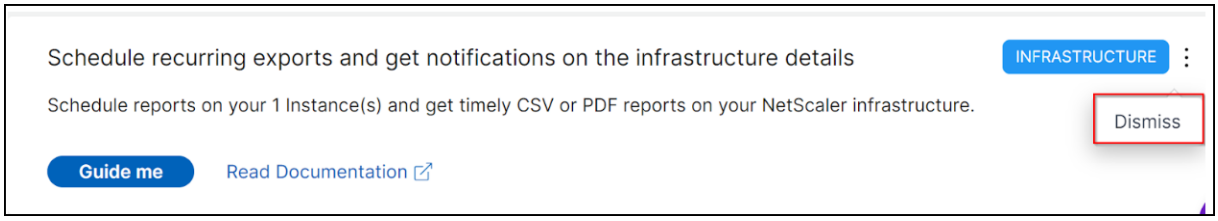
1. 

2. 

3. 

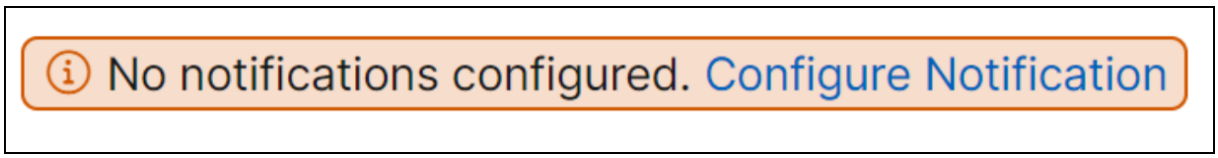
选择分析类型并单击“保存分析”后，建议已完成并移至“已完成”。

同样，如果您想稍后完成任何建议，则可以从列表中选择“驳回”，然后将其移至“已驳回”。



配置通知

每当 NetScaler 控制台发现任何需要您立即执行的未完成任务时，您就可以配置和接收通知。如果您尚未配置通知，则可以单击右上角的 配置通知。



在“通知”页面中，您可以为 Email 和 **Slack** 配置文件，然后单击“保存”以接收通知。对于每种通知类型，NetScaler 控制台 GUI 会显示已配置的分发列表或配置文件。NetScaler 控制台向选定的分发列表或配置文件发送通知。

常见问题解答

1. 引导我不显示工具提示，只显示界面重定向？我该怎么做才能解决这个问题？

   如果您的防火墙阻止 Pendo FQDN，则可能会发生此问题。请参阅为企业启用 Pendo 并确保在防火墙中允许 FQDN。允许 Pendo FQDN 可以让引导我显示工具提示。只有在 Pendo 可用时，您才能以最佳状态体验引导我工作流程。

2. 为什么会向管理员提供此类推荐？

   目前，这些建议是专门针对部署的，可帮助管理员更多地了解配置和设置任务，从而提高部署效率。它还可以更好地发现产品，管理员无需任何先验知识或不知道 NetScaler 控制台中是否存在该功能即可知道任务的作用以及如何提供帮助。

3. 如果我拒绝任何建议会怎样？

   您驳回的建议将移至“已 驳回”。您可以稍后完成这些建议。

4. 如果我开始指导我然后把它放在中间，那么建议会变成 已完成 吗？

   否，除非操作已保存或完成，否则建议不会完成。

5. 我可以进行搜索或筛选吗？

   是！您可以使用搜索栏或通过从列表中选择类别来缩小到特定任务。

6. 我会让任务对动态事件采取操作吗?

   是！目前，您总共可以查看 4 个可操作的任务。有关更多信息，请参阅 任务。

7. 即使我没有在 NetScaler 控制台中添加 NetScaler 实例，所有可操作的任务和 20 多个建议也会显示出来吗?

   没有。您必须在 NetScaler 控制台中同时提供 NetScaler 实例和虚拟服务器，才能显示所有任务和建议。

8. 任务多久刷新一次?

   当您从左侧导航窗格中单击“任务”时，它们会刷新并处于最新状态。详细信息已获取并更新。

用于查看实例关键指标详细信息的统一控制板

January 29, 2024

在 NetScaler 控制台中，您可以查看有关应用使用和性能、NetScaler 基础架构、安全（机器人和 WAF）违规行为等的各种见解。作为管理员，您可能需要导航到 NetScaler 控制台 GUI 中的各种选项才能查看多个见解。例如，要查看虚拟服务器（应用程序）和 NetScaler 实例见解：

- 您必须先导航到 应用程序 **>** 控制板 才能查看应用程序的见解。
- 然后，您必须导航到 基础架构 **>** 基础架构分析，以查看 NetScaler 实例的见解。

为了获得更好的监视体验，您必须拥有包含所有所需见解概述的权限。导航到 概述 **>** 控制板，可视化单窗格控制板，其中包含基于以下类别的关键指标详细信息概述：

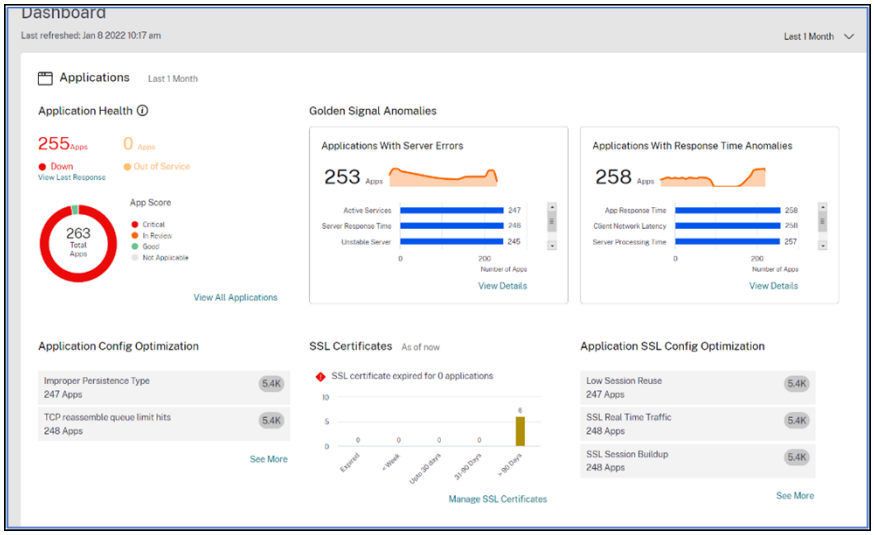
- 应用程序
- NetScaler 基础架构
- 应用程序安全性
- 网关
- API 分析

应用程序

在“应用程序”下，您可以查看：

- 应用程序运行状况-根据其状态（例如“严重”、“正在 ** 审核”、“良好”和“不适用”）概述处于停机和停止运行状态的应用程序。单击“查看所有应用程序 **”以在应用程序控制面板中查看详细信息。
- 黄金信号异常—概述存在服务器错误和响应时间异常的应用程序。单击 **View Details**（查看详细信息）了解更多信息。

- 应用程序配置优化 -概述存在性能问题的应用程序总数。单击“查看更多”可在应用程序控制面板中查看问题详情。
- **SSL** 证书 -提供 SSL 证书及其有效性的概述。单击“管理 **SSL** 证书”可在 SSL 控制面板中查看更多信息。
- 应用程序 **SSL** 配置优化 -概述存在 SSL 相关问题的全部应用程序。单击“查看更多”查看问题详情。



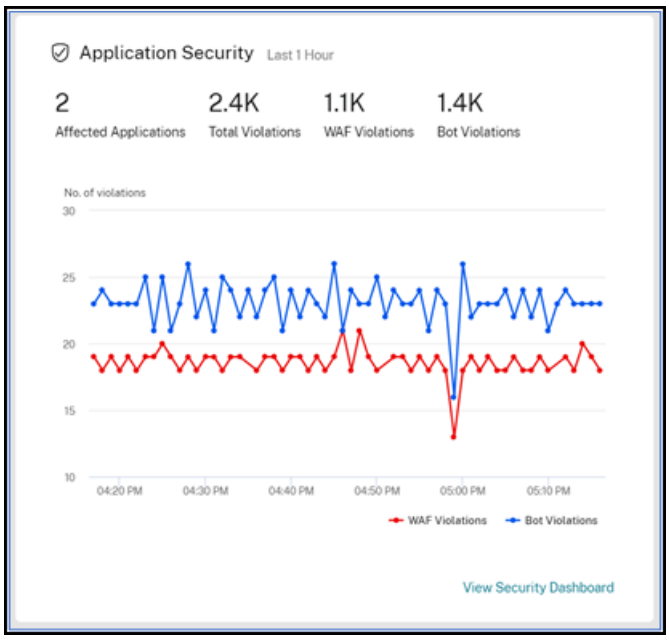
NetScaler 基础架构

在 **NetScaler** 基础架构下，您可以查看以下与 NetScaler 实例相关的关键指标：

- **NetScaler** 实例运行状况—根据实例 评分概述 NetScaler 实例总数。
- 受 **CVE** 影响的 NetScaler 实例—概述受 常见漏洞和暴露 (CVE) 影响的 NetScaler 实例总数。有关更多信息，请参阅 安全公告。
- **NetScaler** 实例 问题—根据问题类别概述 NetScaler 实例问题。有关更多信息，请参阅 基础结构分析
- **NetScaler** 实例升级摘要—概述非最新版本的 NetScaler 实例总数。单击“查看 **NetScaler** 实例 控制面板”以了解更多信息。

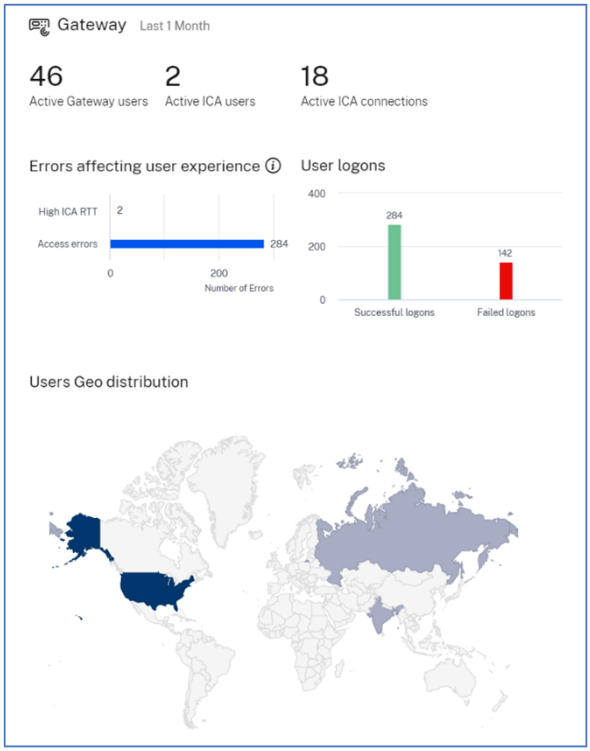
应用程序安全性

概述选定持续时间内报告的受影响应用程序总数和违规总数（Bot 和 WAF）。单击“查看安全控制面板”以查看安全和机器人违规的详细信息。



网关

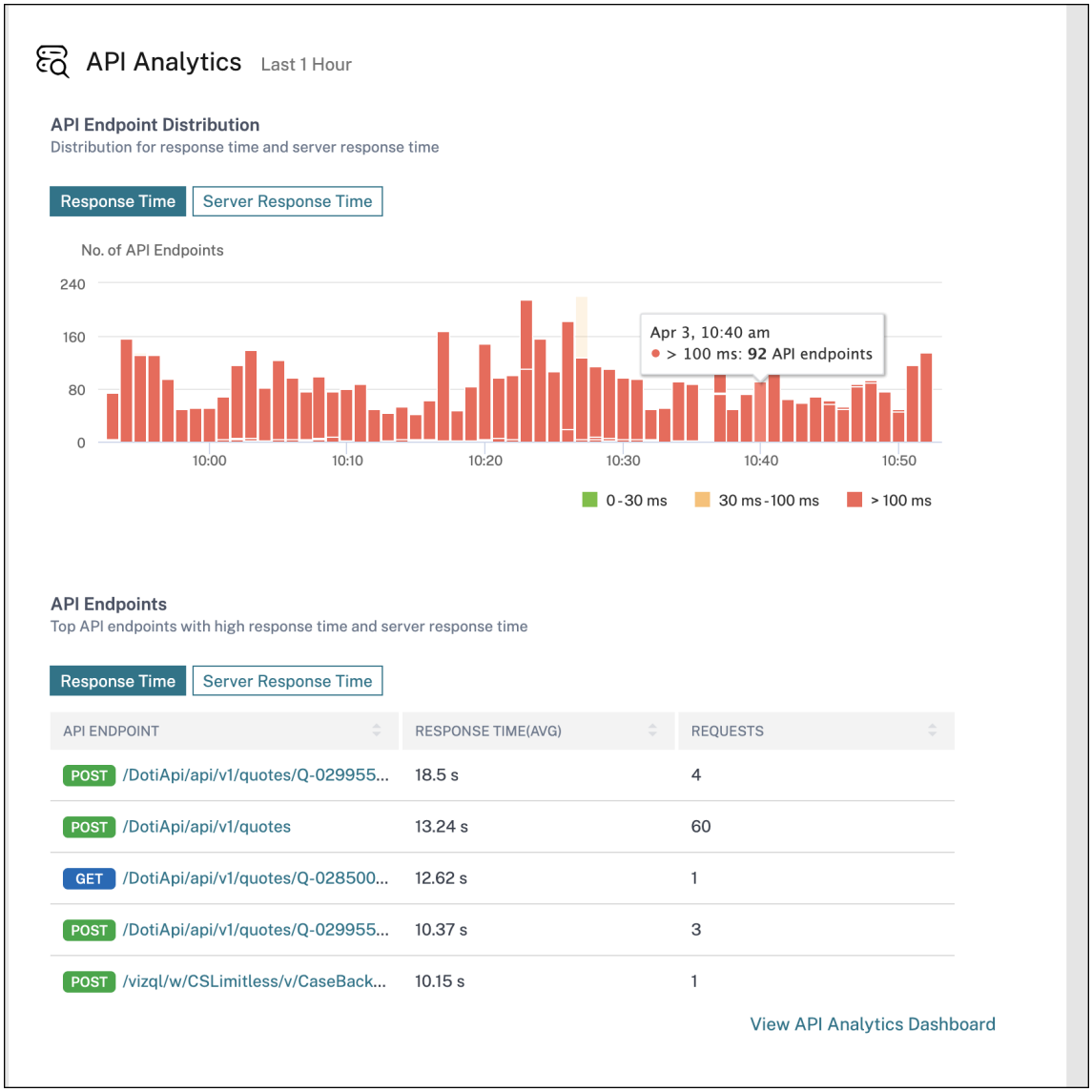
提供活跃网关用户总数、活跃 ICA 用户总数和活跃 ICA 连接总数的概述。您还可以查看错误、用户登录详细信息以及提供用户位置详细信息的地理地图。



API 分析

概述了通过 NetScaler 控制台配置的 API 端点的性能和使用情况。您可以查看：

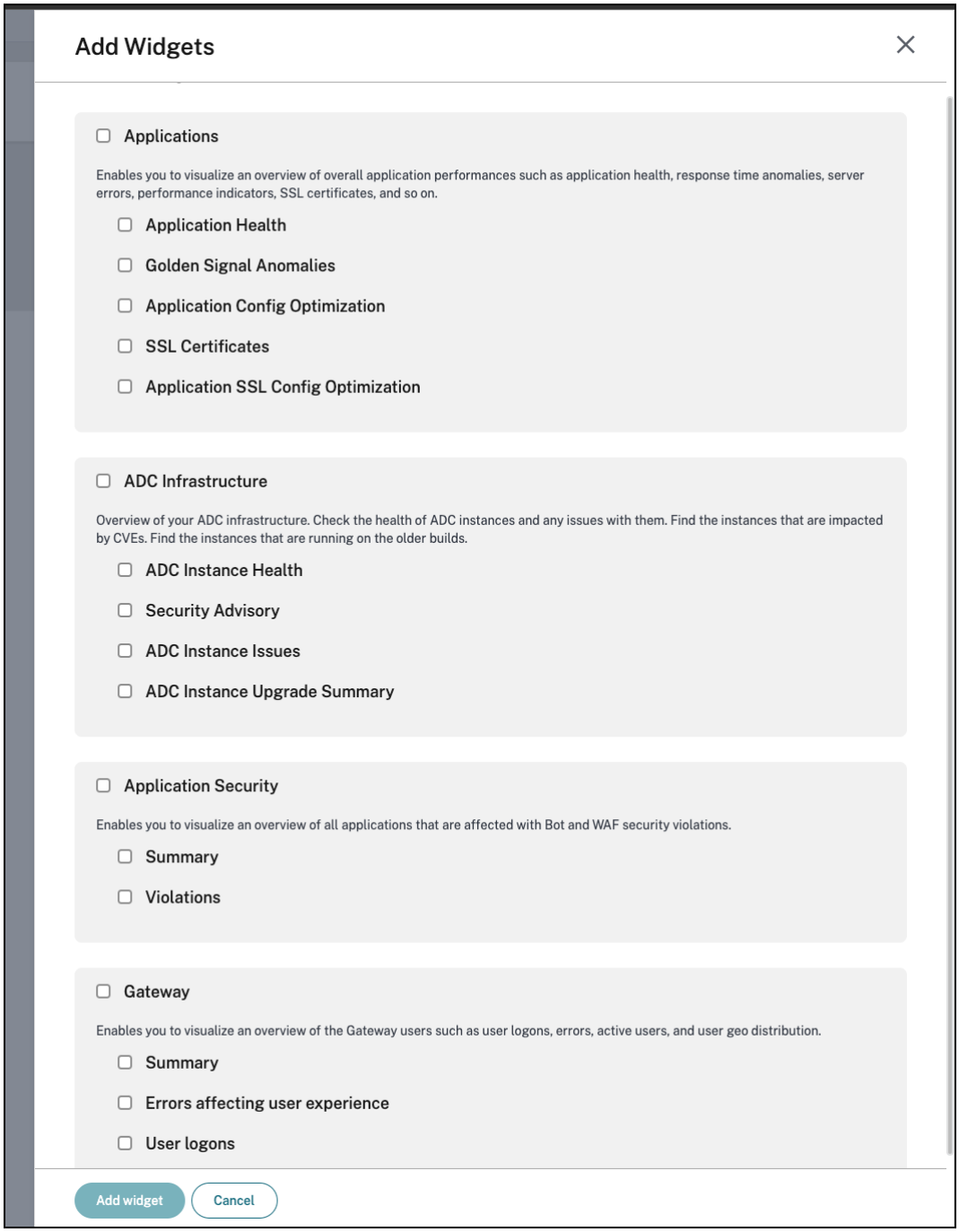
- API 端点的应用程序和服务器响应时间分布。
- 应用程序和服务器响应时间较长的端点。



自定义控制面板

您可以使用“编辑控制板”选项，并根据您的选择自定义控制板视图。使用“编辑控制板”选项，您可以：

- 拖动小部件
- 移除整个控件（应用程序、NetScaler 基础架构、网关或应用程序安全）。
- 移除每个控件下方的较小部件。
- 单击“添加小组件”，然后在每个小组件下选择要查看的所需关键指标。



- 重置为默认值
- 重置为上次保存

进行更改后，单击“保存”。

> 注意
>
> - 默认情况下，显示所有小部件。如果您自定义控制板，保存更改，然后再次使用“重置为默认值”选项，则

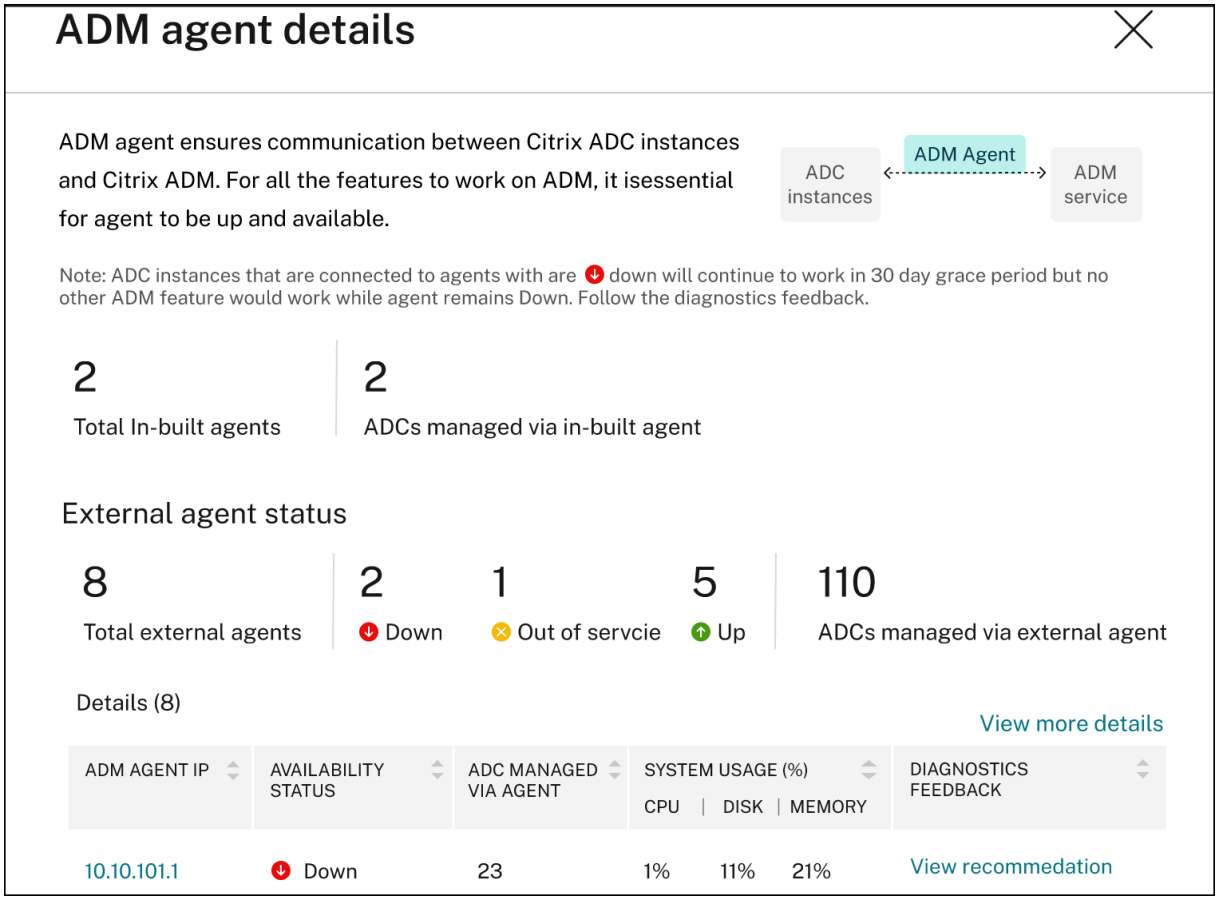
> 所有小部件都将添加到控制板中。
>
> - 重置为上次保存的选项加载先前保存的配置。

查看代理详情

在统一的控制板中，您可以可视化代理详细信息的概述。在 代理状态旁边的 概述 **>** 控制板中，您可以查看以下状态，从而可以分析整体代理可用性：

- 全部可用。表示所有代理均已启动并正在运行。
- 全部不可用。表示所有代理均已关闭且无法访问。
- **[**代理数量**]** 不可用。表示有几个代理已关闭且无法访问。
- 全部已停止服务。表示所有代理均已停止服务。
- **[**代理数量**]** 已停止服务。表示有几个代理已停止服务。
- 未找到外部代理。表示未配置代理（通过任何虚拟机管理程序）。

单击“查看详细信息”可视化代理详细信息的概述，例如内置代理总数、外部代理总数、代理 IP、状态、系统使用情况、诊断检查等。



创建和应用过滤器

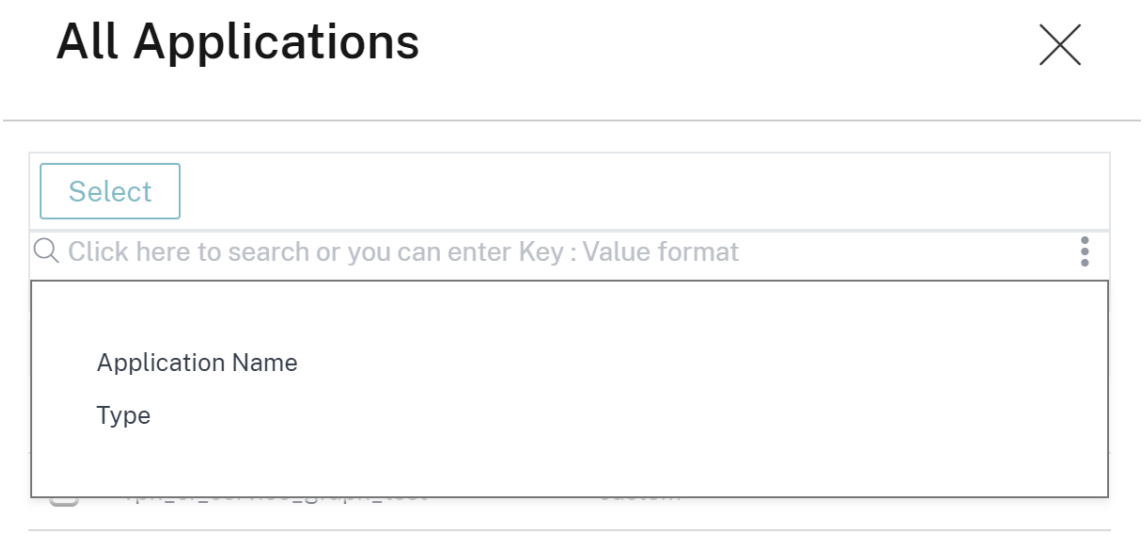
您只能对以下所选实例或应用程序应用过滤器和查看见解：

- 应用程序
- NetScaler 基础架构
- 应用程序安全性

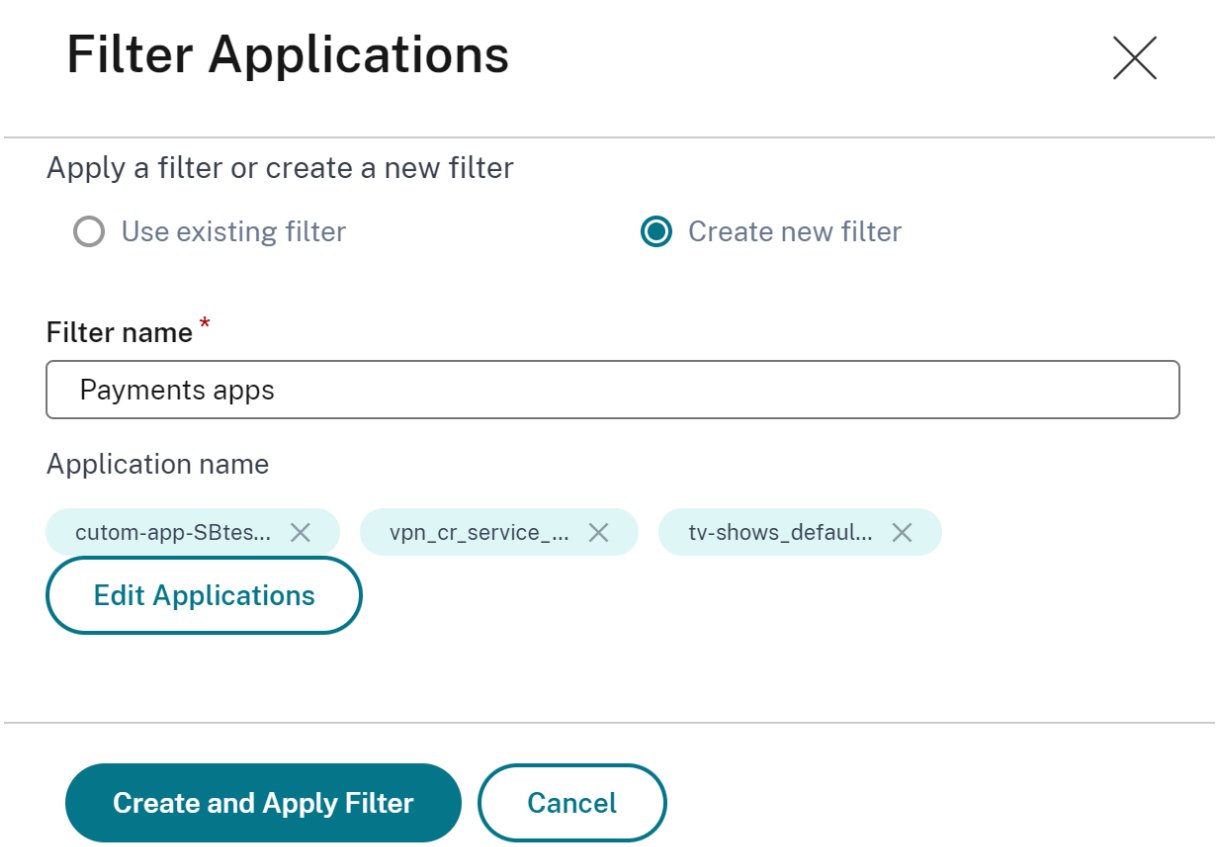
默认情况下，所有应用程序都处于选中状态。您可以通过单击磁贴中可用的筛选器图标从控制板创建自定义文件管理器。

在“筛选应用程序”窗口中：

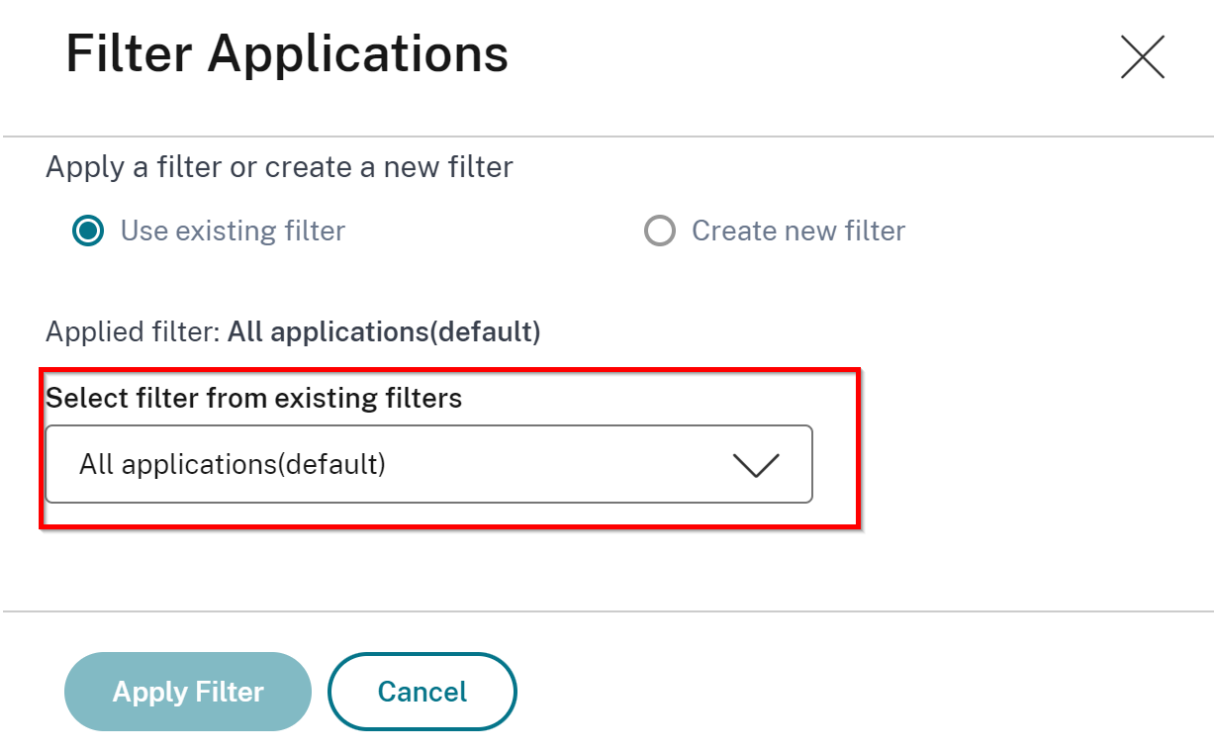
1. 选择“创建新过滤器”。
2. 根据您的选择提供过滤器名称。
3. 单击“选择应用程序”，然后为过滤器添加所有必需的应用程序。选择应用程序时，也可以使用筛选器（应用程序名称和类型），然后选择应用程序。



4. 单击“创建并应用过滤器”。

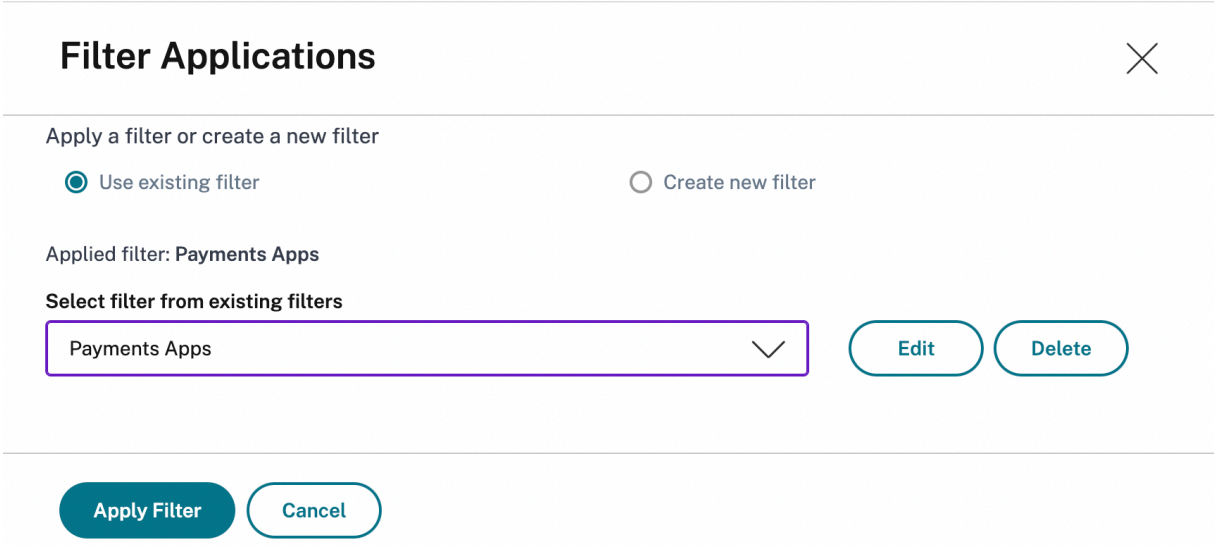


过滤器现已创建并应用。您可以按照相同的步骤创建更多过滤器。创建筛选器后，您可以通过“从现有筛选器中选择过滤器”列表选择和应用过滤器。



编辑过滤器

您可以通过从列表中选择过滤器并单击“编辑”来编辑过滤器。使用编辑选项，您可以添加或删除应用程序，然后更新过滤器。



要删除筛选器，请从列表中选择该过滤器，然后单击“删除”。

> 注意
>
> 当您使用应用程序创建过滤器时，如果在应用程序控制板中删除了其中一个应用程序，则应用程序详细信息将立即从统一控制板中删除。

创建自定义控制板以查看实例密钥指标详情

January 29, 2024

与统一控制板（概述 **>** 控制板）类似，您可以根据自己的选择通过创建自定义控制板来查看实例指标详细信息。通过为每个控制板使用唯一的名称，您最多可以创建 20 个控制板。作为管理员，此增强功能使您能够创建多个控制板并仅监视所需的实例见解。

首先，请考虑您要监视应用程序和应用程序安全的关键指标：

1. 导航到 概述 **>** 自定义控制板。
2. 单击 **+** 创建新的控制板。

   在“创建自定义控制板”页面中：

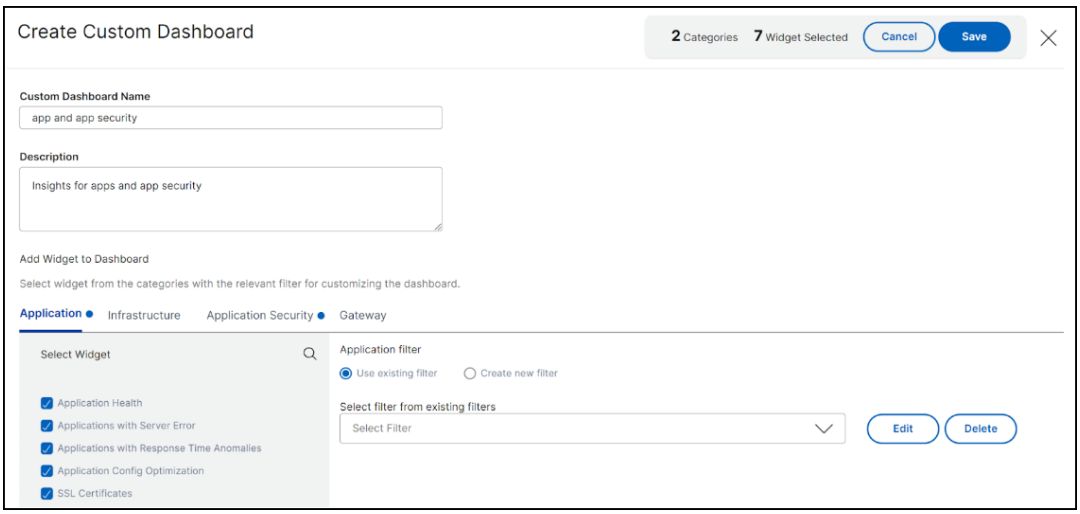
   a) 自定义控制板名称 -为控制板指定一个唯一的名称。

   b) 说明 -提供简短描述以获得更多详细信息。

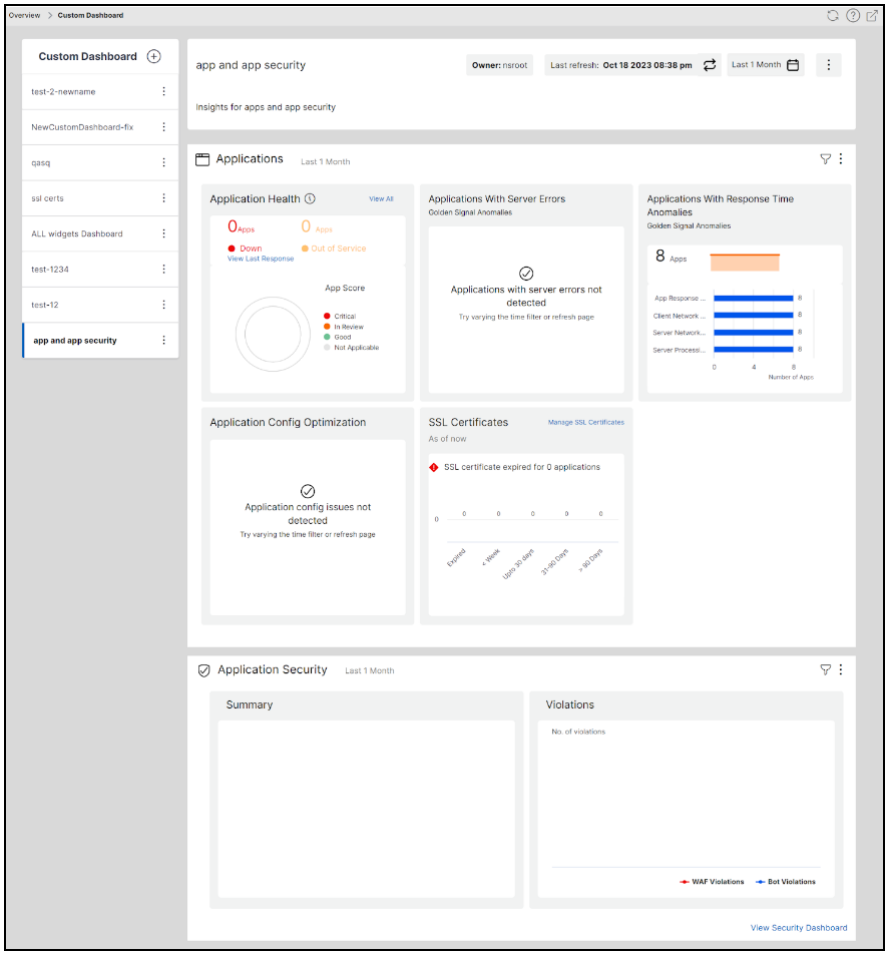
   c) 将控件添加到控制板 -在本示例中，要求为应用程序和应用程序安全添加小部件。从“应用程序”和“应用程序安全”类别中选择要监视的小组件。

   d) 应用程序过滤器 -默认情况下，过滤器应用于所有应用程序。您也可以创建过滤器并仅选择特定的应用程序。有关更多信息，请参阅 创建和应用过滤器。

   e) 单击保存。

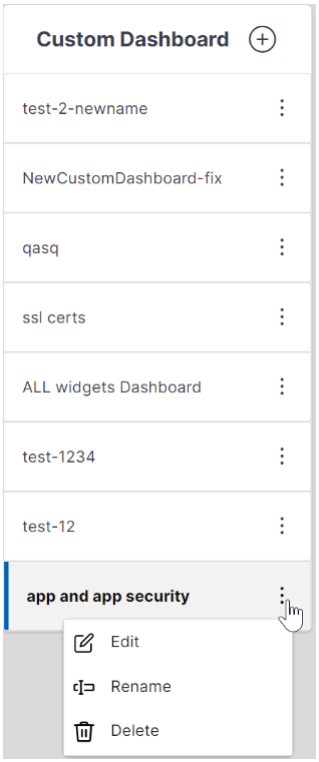


控制板已成功创建。同样，您可以创建多达 20 个控制板，并通过为每个控制板指定一个唯一的名称来根据自己的选择选择类别。



创建自定义控制板后，您可以使用以下选项：

- 编辑：您可以通过添加更多小部件或删除小部件、应用筛选器等来编辑控制板。
- 重命名：您可以更改控制板名称。
- 删除：您可以删除控制板。

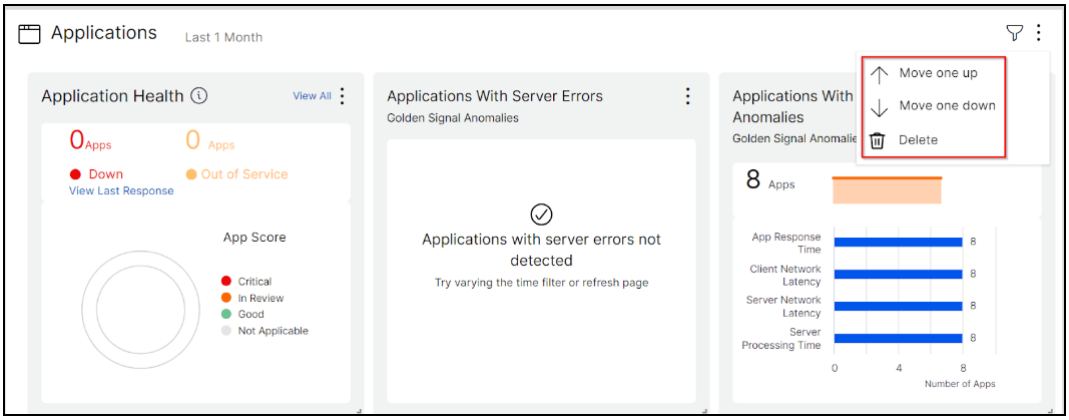


控制板中有更多选项

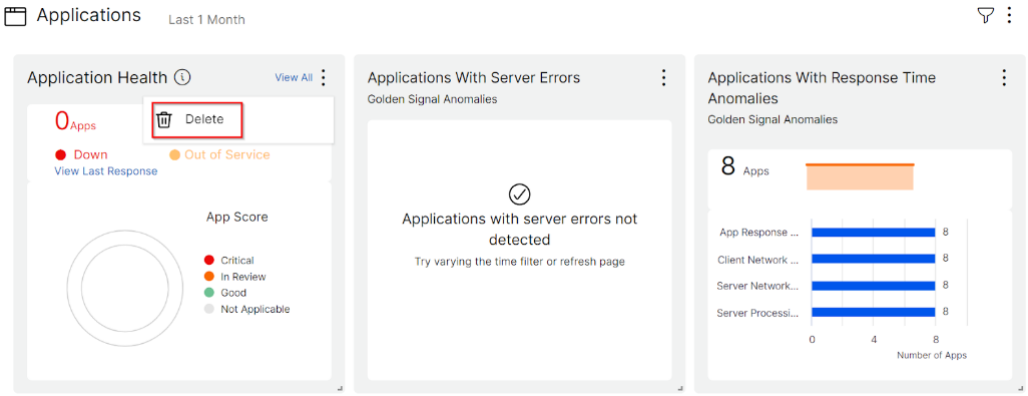
在您创建的自定义控制板中，您可以使用以下选项：

(更多选项)

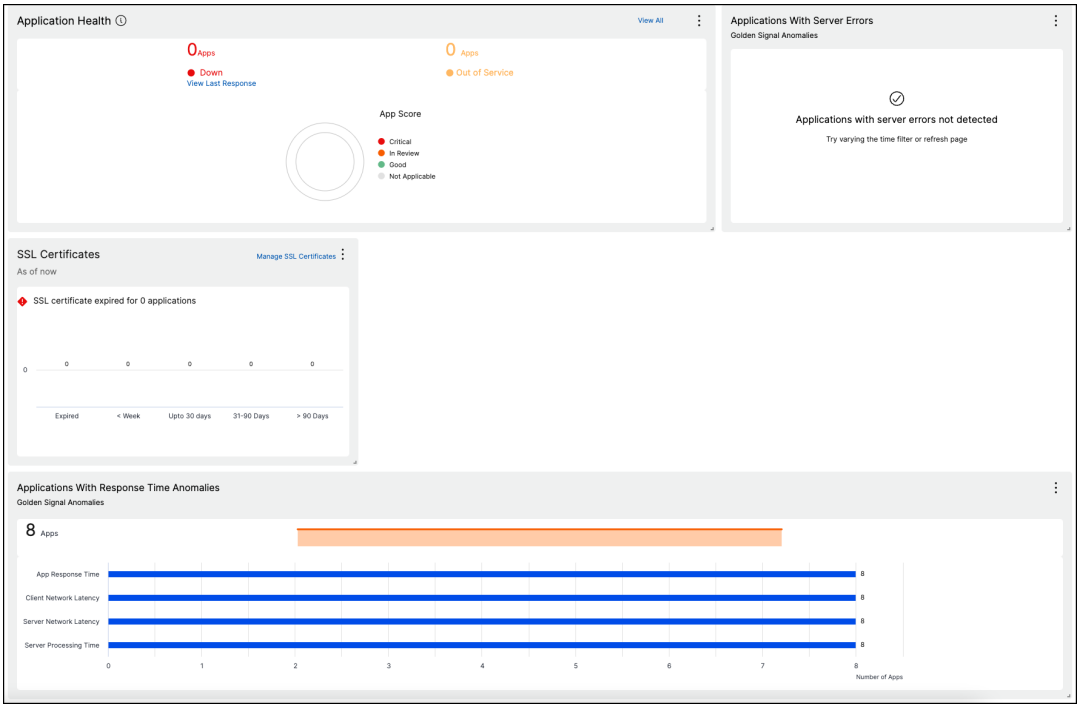
- 编辑配置：您还可以使用此选项通过添加更多小组件或删除小部件、应用筛选器等来编辑控制板。
- 编辑布局：您可以使用此选项对控制板进行其他自定义。
  - 您可以选择向上移动、向下移动或删除。



- 在控件中，您可以通过选择“删除”选项来删除任何控件。



- 拖放即可将小部件放置在任何您想要的地方。
- 增加或减小控件的大小，以更好地了解某些见解。



进行更改后，单击“保存”以查看更新的控制板。

将控制板共享给其他用户

您可以将控制板共享给其他用户。选择现有控制板，然后单击“共享”。键入用户名，然后单击“邀请”以共享控制面板。分配的用户可以在只读模式下查看控制板。

API 安全性

January 29, 2024

API 或应用程序编程接口是一组规则、协议和工具，允许不同的软件应用程序或系统相互通信。API 通过强制执行访问控制、身份验证和加密，确保只有授权实体才能安全地访问和传输机密信息，在保护敏感数据方面发挥着重要作用。

API 可用作移动和 Web 应用程序的后端框架。因此，保护它们传输的敏感数据至关重要。API 安全性是指防止或缓解针对 API 的攻击的做法。

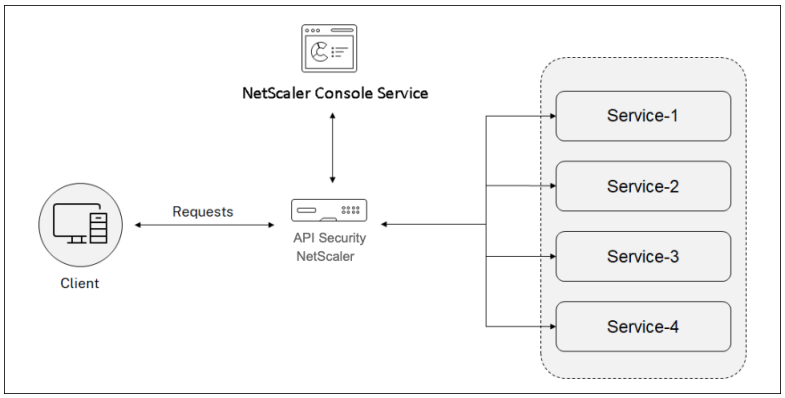
在 API 安全性中，网关充当向 API 端点发出的所有请求的入口点。此外，还可确保安全可靠地访问系统中的所有 API 端点和微服务。

要保护您的 API，请执行以下步骤：

- 创建或上载 API 定义

- 部署 API 实例
- 将策略添加到 API 部署

下图描述了 NetScaler 控制台中的 API 安全如何接收客户端请求并发送来自后端 API 服务的响应：



> 注意：
>
> 在 NetScaler 控制台中，拥有高级或高级许可的用户可以使用此功能。

API 安全性的好处

API 安全性为您提供了以下好处：

- 保护您的 **API** 端点：API 安全性增加了安全层，它可以保护您的 API 端点和后端 API 服务器免受攻击，例如：
  - 缓冲区溢出
  - SQL 注入
  - 跨站点脚本
  - 拒绝服务 (Dos)
- 监视和改进 **API** 性能：API 安全性提供 SSL 卸载、身份验证、授权、速率限制等服务。这些服务提高了 API 性能及其可用性。

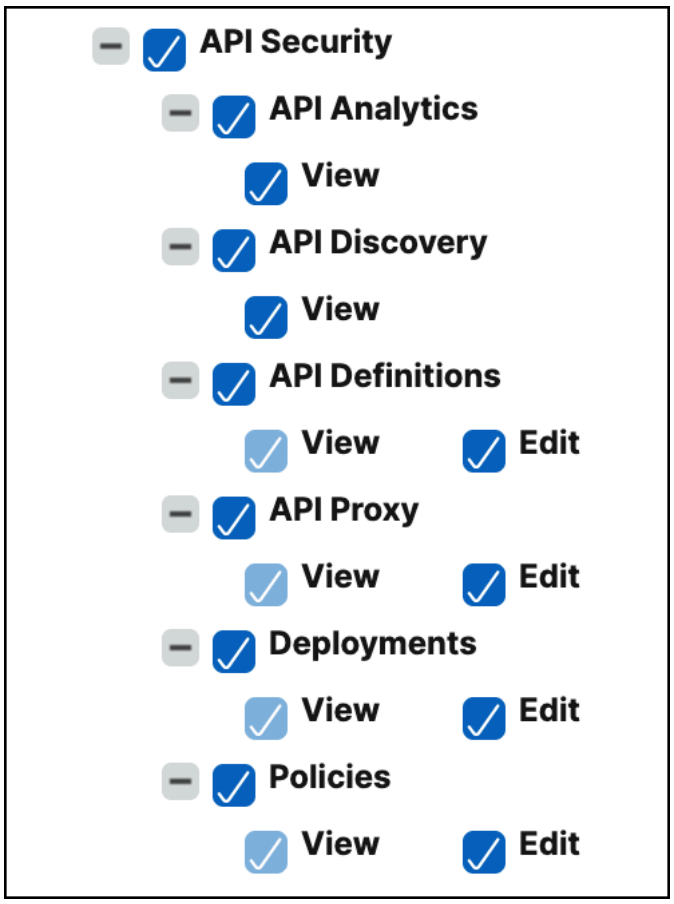
  API 分析为您提供 API 性能指标和 API 端点所面临的威胁的可见性。有关更多信息，请参阅 查看 API 分析。
- 管理 **API** 流量：API 安全性抽象了您的后端 API 基础设施的复杂性。
- 发现 **API** 端点：API 安全性会发现您组织中的 API 端点并添加到 **API** 发现页面。

授予 API 安全性配置和管理权限

作为管理员，您可以创建访问策略来授予用户进行 API 安全性配置和管理的权限。用户权限可以是查看、添加、编辑和删除。执行以下操作以授予权限：

1. 导航到“设置” > “用户和角色” > “访问策略”。

2. 单击添加。
3. 在 创建访问策略中，指定策略名称和描述。
4. 在“权限”字段中，展开“应用程序”，然后展开 **API** 安全性。
5. 选择所需的 **API** 安全性页面。然后，选择要授予的权限。



> 重要：
>
> 确保为使用 API 安全性所需的功能授予权限。例如，如果您授予用户访问“部署”页面的权限，则以下功能还需要用户访问权限：
>
> - 样书
> - IPAM
> - 负载平衡（在 网络功能下）
> - 内容切换（在 网络功能下）
> - 设备 API 代理（在 **API** 下）

有关访问策略的更多信息，请参见 在 NetScaler 控制台上配置访问策略。

创建或上载 **API** 定义

January 29, 2024

API 定义是使用 OpenAPI 规范标准（Swagger 2.0、OpenAPI 3.0.x）描述 API 的文档。此定义可以包含 API 资源路径和操作它们的方法。您可以将 API 定义添加到 NetScaler 控制台，然后将其部署到 API 网关（NetScaler）。

您可以通过以下方式之一创建 API 定义：

- 上载 Swagger OAS 规范文件
- 创建您自己的 API 定义

> 注意：
>
> 目前，NetScaler 控制台支持解析 使用 **Swagger 2.0** 或 openapi 3.0.1** 的 OAS 规范文件。

上载 **OAS** 规范

您可以将 OAS 规范上载到 NetScaler 控制台 GUI。

1. 导航到“安全性”**>**“**API** 安全性”**>**“**API** 定义”。
2. 单击添加。
3. 选择 上载 **OAS** 规范。

   > 注意：
   >
   > 确保 OAS 规范文件采用 YAML 或 JSON 格式。而且，此文件不得包含外部引用。目前，NetScaler 控制台支持 Swagger 版本 2.0。

4. 在本地电脑上浏览 OAS 规范，然后上载到 NetScaler 控制台。

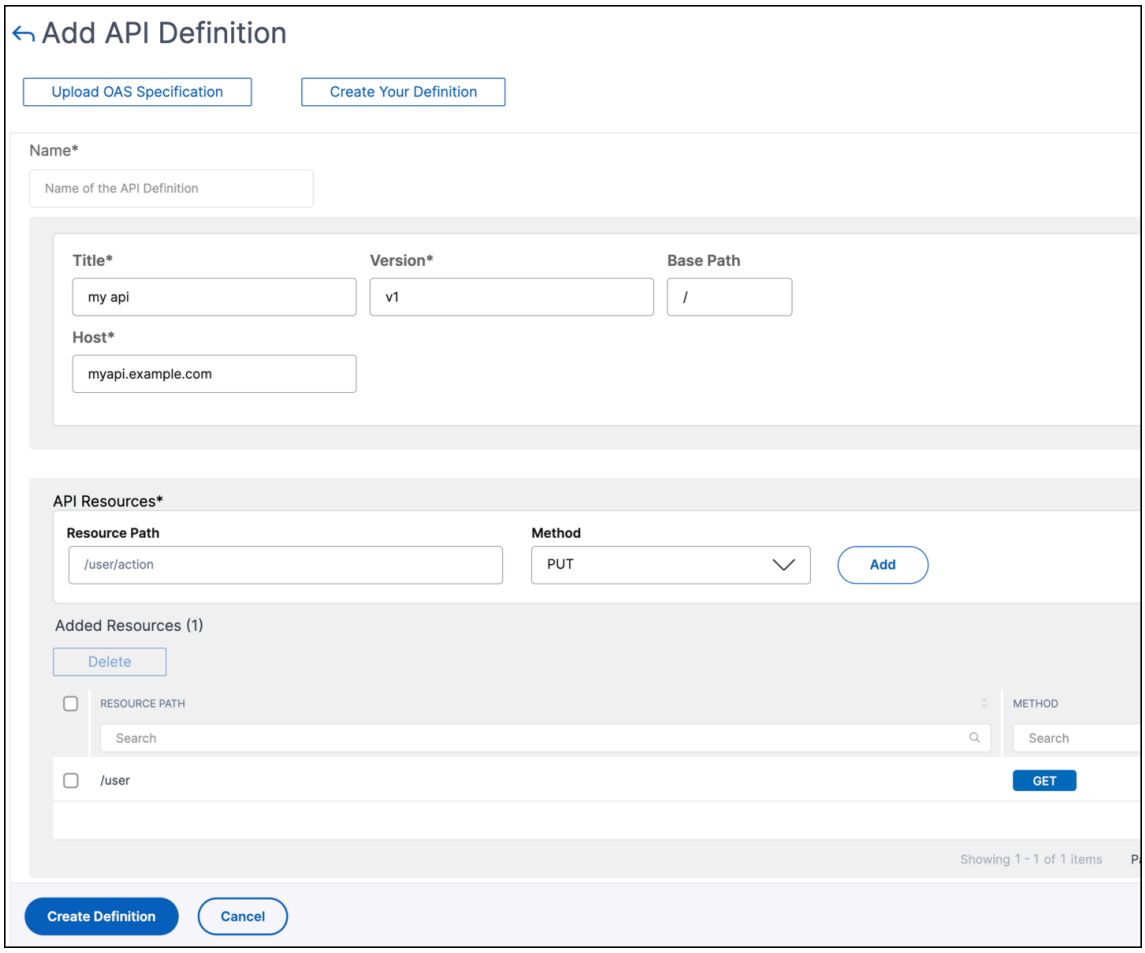
创建 **API** 定义

您可以在 NetScaler 控制台 GUI 中创建自己的 API 定义。

1. 导航到“安全性”**>**“**API** 安全性”**>**“**API** 定义”。
2. 单击添加。
3. 选择 创建定义 并指定以下内容：

   - 名称 -API 定义的名称。
   - **API** 定义 -定义必须包括标题、版本、基本路径和主机。您可以在 主 机字段中指定域名或 IP 地址。

- **API** 资源 -向定义中添加多个 API 资源。每个资源都有一个路径和支持的方法。单击添加。该资源将添加到“已 添加的资源”表中。单击“删除”删除 API 资源。



4. 单击创建。

查看 **API** 定义

“**API** 定义”页面列出了上载的定义。单击“查看”可查看 以下 API 定义的详细信息：

- 名称 -显示 API 定义的名称。
- **API** 定义 -显示定义的标题、版本、基本路径和主机。
- **API** 资源—列出 API 定义中的 API 资源及其操作方法。

部署 **API** 实例

January 29, 2024

要部署 API 实例，您需要一个 API 代理。API 代理是一个前端虚拟服务器，API 安全性（NetScaler 实例）在其中接收来自 API 客户端的 API 流量。API 客户端可以是浏览器、移动应用程序等。

您可以与不同的 API 部署共享 API 代理。在拥有许多 API 服务的组织中，您可以为每个 API 服务创建单独的 API 代理。或者，您可以创建一个 API 代理并将其与不同 API 服务的 API 实例共享。

例如，两个 API 服务 `app1` 和 `app2` 部署在相同的 API 安全性上并使用相同的前端虚拟服务器。您希望向两个 API 服务提供相同的虚拟 IP 地址和 SSL 证书信息。在这种情况下，您可以添加具有所需信息的 API 代理，并与单独的部署共享。因此，不同部署上的 API 服务可以使用共享 API 代理接收请求。

作为管理员，执行以下操作来部署 API 实例：

1. 添加 API 代理。
2. 使用 API 代理部署 API 实例。

添加 **API** 代理

按照以下步骤添加 API 代理：

1. 前往“安全性”**>**“**API** 安全性”**>**“**API** 代理”**>**“添加”。
2. 指定以下内容：
    - 代理名称—API 代理的名称。
    - 目标 **NetScaler** 实例-选择用作 API 网关的 NetScaler 实例。
    - **IP** 地址 -托管 API 服务的虚拟服务器的 IP 地址。
    - 端口 -托管 API 服务的虚拟服务器的端口号。
    - 协议 -根据您希望在 API 代理上接收的流量类型设置协议（HTTP 或 HTTPS）。
    - **TLS** 安全配置文件 -从列表中选择高或中。如果您选择“高”，它将映射到 NetScaler 实例上的 A+ 等级 SSL 配置文件。
    - 证书存储 -为 API 安全性选择 SSL 证书。NetScaler 代理证书存储可帮助您在一个位置存储和管理 SSL 证书。

      在 NetScaler 代理证书存储库中，您可以将 SSL 证书存储在 NetScaler 代理中，并在配置 NetScaler 期间重复使用它们。

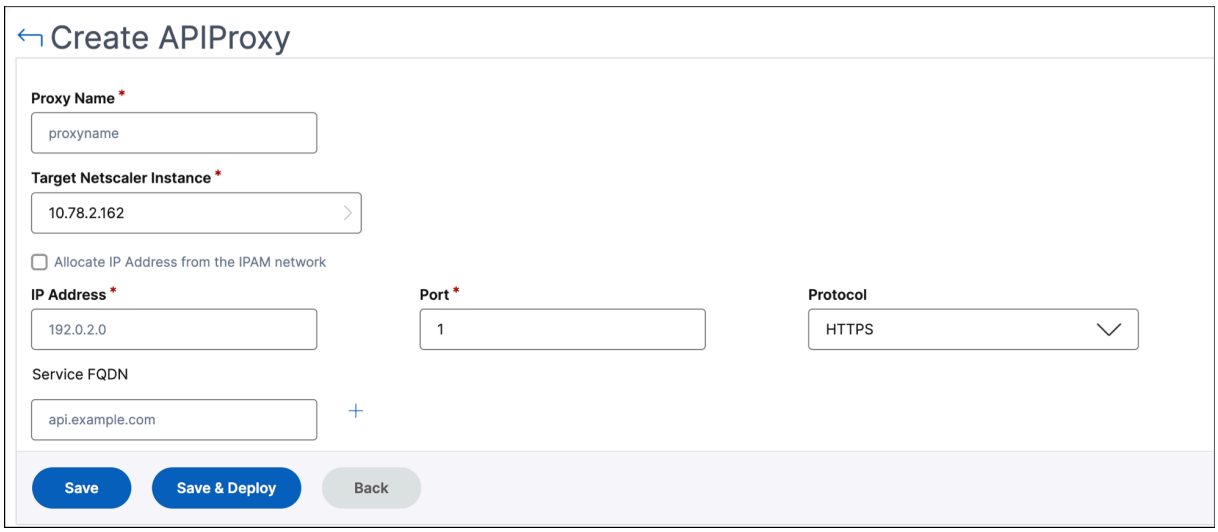
      > 注意：
      >
      > 如果您的现有部署使用不在 NetScaler 代理证书存储库中的 SSL 证书或密钥，则必须使用相同名称将证书和密钥添加到存储中。

    - 服务 **FQDN** -托管 API 服务的完全限定域名。例如：`api.example.com`

或者，您可以选择 IPAM 网络来分配 IP 地址。要查看从 IPAM 网络分配的 IP 地址，请导航到 设置 **> IPAM**。有关 IPAM 的更多信息，请参阅 配置 IPAM。

3. 单击 保存 以保存部署配置。

   如果要在 API 安全性上部署此 API 代理，请单击“保存并部署”。



添加 API 代理后，部署 API 实例。

使用 **API** 代理部署 **API** 实例

按照以下步骤部署 API 实例：

1. 导航到 安全性 **> API** 安全性 **>** 部署。
2. 单击添加。
3. 在“部署基本 信息”中，

   a) 指定 部署名称。

   b) 在 **API** 定义中，选择所需的 API 定义。

   c) 选择要用于此部署的 **API** 代理。

4. 在“上游服务”中，单击“添 加”以添加要将 API 流量输出 API 流量的后端（源）API 服务器。您可以使用其域名或 IP 地址配置上游服务。

   在部署 API 实例时，您可以指定 SNIP 地址和网络掩码详细信息。NetScaler 实例使用指定的 SNIP 地址与上游服务（后端）通信。指定的 SNIP 地址成为发送到上游服务的出口流量的源 IP 地址。您也可以使用 IPAM 配置 SNIP 地址和网络掩码。如果您未配置 SNIP 地址，则 NetScaler 实例的默认 SNIP 地址将成为上游服务的源 IP 地址。

> 注意：
>
> 默认情况下，截图地址和网络掩码选项是可选的。但是，如果您指定其中一个选项，则还必须指定另一个选项。

a) 为上游服务指定一个名称。

b) 指定域。

c) 在 服务中，指定 IP 地址和端口值。要添加更多 IP 地址，请单击“添加新行”。

d) 单击添加。

5. 在 路由中，指定以下详细信息以根据资源路径前缀路由传入的 API 流量：

a) 指定路径名称。

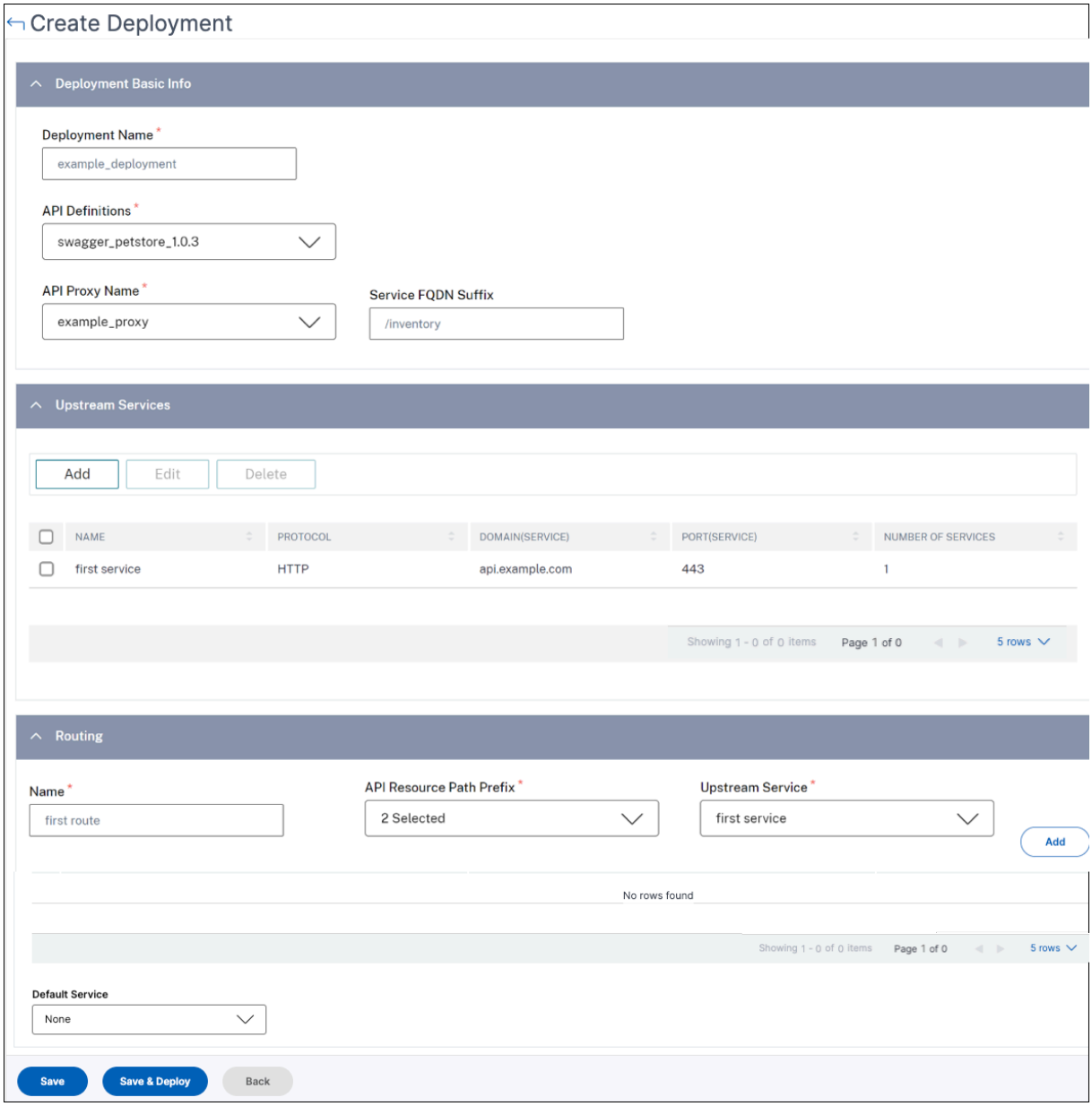
b) 选择一个 **API** 资源 来接收 API 请求。

> 注意：
>
> 您也可以指定自定义路径或路径前缀。

c) 从列表中选择要在其中传输 API 流量的 上游服务。

6. 单击 保存 以保存部署配置。

如果要将配置部署到 API 安全性，请单击“保存并部署”。



启用 **API** 分析

以下是为部署启用分析的先决条件：

- 确保虚拟服务器已获得许可
- 确保分析状态为“已禁用”
- 确保虚拟服务器处于运行状态

要为部署启用 API 分析，请执行以下操作：

1. 在“安全”**>**“**API** 安全性”**>**“部署”中，选择要启用 API 分析的部署。

2. 单击 启用分析。
3. 在 为部署配置 **Analytics** 页面中，选择虚拟服务器，然后单击 启用 **Analytics**。
4. 在 启用分析 窗口中：
   a) 选择洞察类型（Web Insight、Security Insight、机器人洞察）
   b) 选择 **Logstream** 或 **IPFIX** 作为传输模式。

      有关 IPFIX 和 Logstream 的更多信息，请参阅 Logstream 概述。

      默认情况下，表达式为真。
   c) 单击确定。

NetScaler 控制台支持对所选虚拟服务器进行分析。

将策略添加到 **API** 部署

January 29, 2024

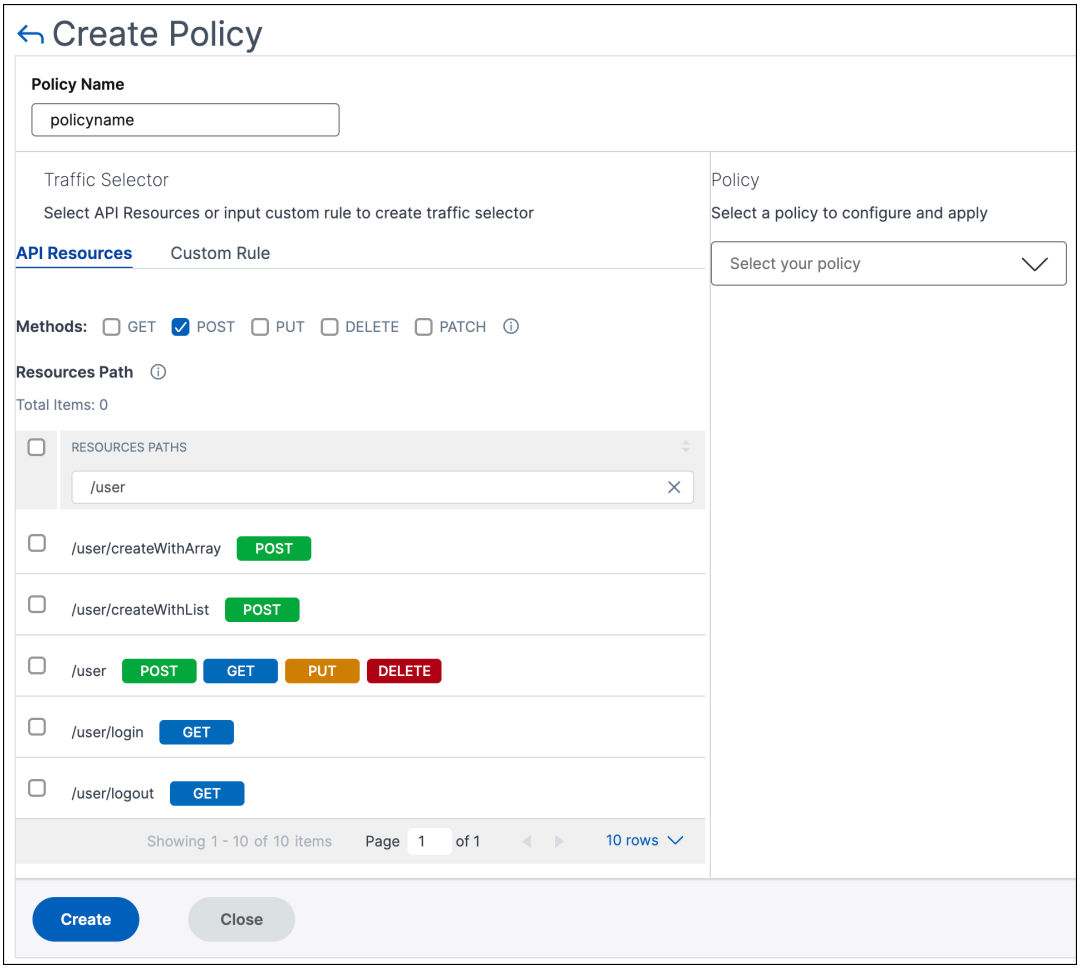
您可以为 API 流量配置各种安全策略。此配置要求您指定策略所需的流量选择标准和参数。执行以下步骤将策略添加到 API 定义：

1. 导航到“安全性”**>**“**API** 安全性”**>**“策略”。
2. 单击添加。
3. 指定策略组的名称。
4. 从列表中选择 部署。
5. 从列表中选择要为其配置策略的 上游服务。
6. 单击 添加 选择通信选择器和策略类型。

   流量选择器 -流量选择标准包括 API 资源路径或路径前缀、方法和策略。

   您可以使用以下任一选项来指定流量选择标准：

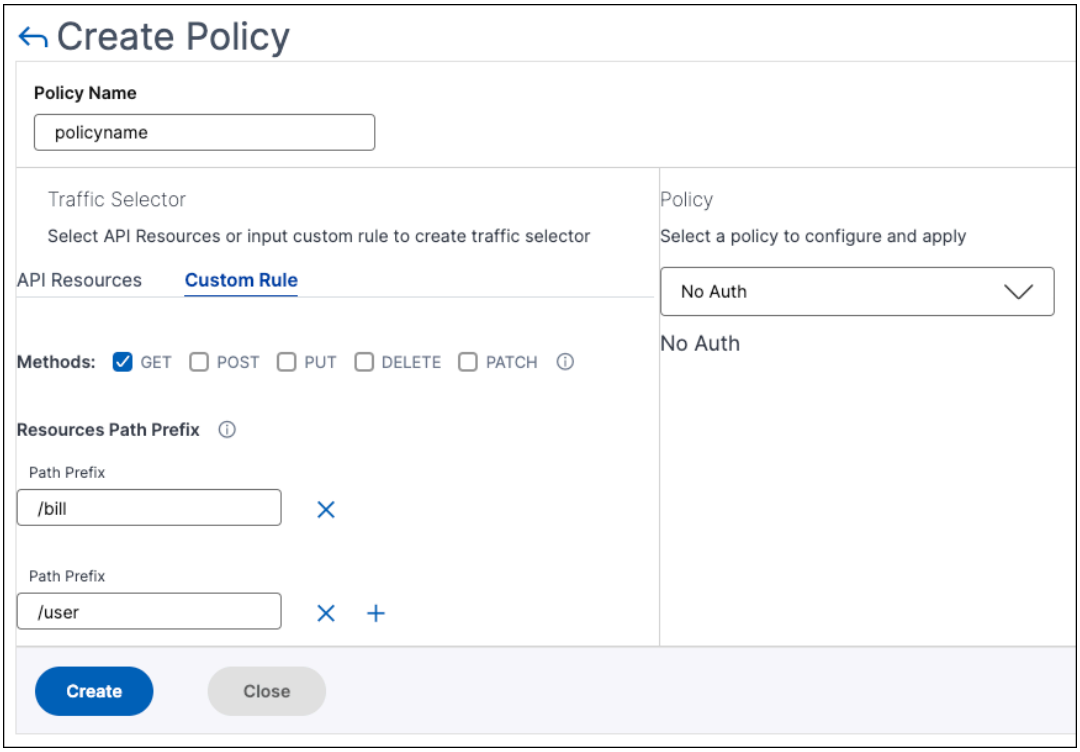
   - **API** 资源—选择要应用策略的 API 资源及其方法。您可以使用关键字搜索 API 资源和方法。



在此示例中，将列出具有 `/user` 该 `POST` 方法的 API 资源。

- 自定义规则—在此选项卡中，您可以指定自定义路径前缀和多种方法。

  配置的策略适用于与 API 流量选择的自定义规则匹配的传入 API 请求。



在此示例中，**No-Auth** 策略适用于具有 `/bill` 前缀和 `GET` 方法的 API 资源。

在 策略中，从列表中选择要应用于所选 API 资源和方法的策略。有关每个策略的更多信息，请参阅 策略类型。

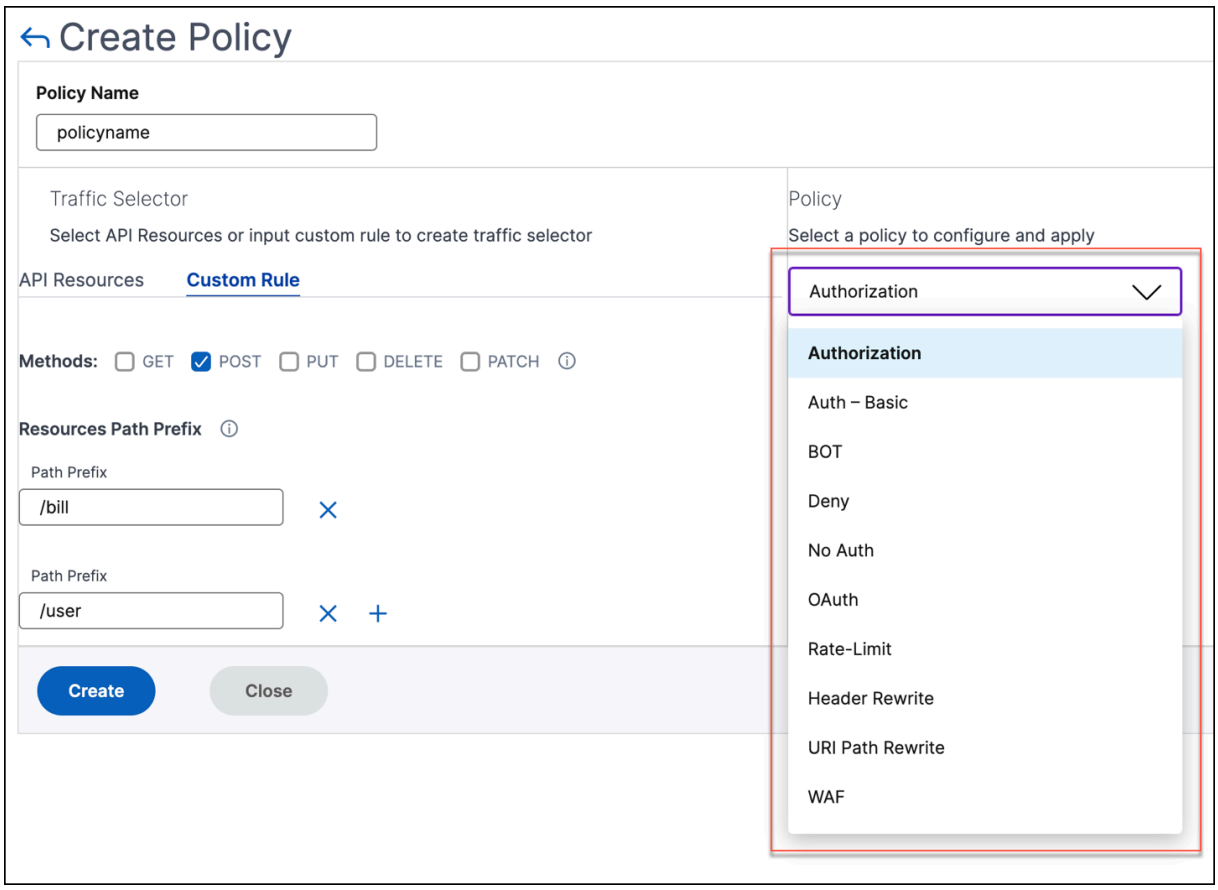
7. 可选，您可以移动策略类型以设置优先级。优先级较高的策略类型首先适用。
8. 单击“保存”添加策略。如果要立即应用策略，请单击“保存并应用”。

策略类型

配置 API 策略时，可以选择要应用于 API 资源和方法的以下策略：

- 身份验证和授权
- 速率限制
- **WAF**
- 机器人
- 标题重写
- **URI** 路径重写
- 拒绝

> 注意：
>
> 要使用 API 管理 API 安全性，请参阅使用 API 管理 API 安全性。



身份验证和授权

API 资源托管在应用程序或 API 服务器上。当您想对此类 API 资源实施访问限制时，可以使用身份验证和授权策略。这些策略验证传入的 API 请求是否具有访问资源的必要权限。

使用以下策略为所选 API 资源定义身份验证和授权：

No-Auth 使用此策略可以跳过对所选流量的身份验证。

Auth-Basic 此策略指定要与 HTTP 基本身份验证方案一起使用的本地身份验证。要使用本地身份验证，必须在 NetScaler 上创建用户帐户。

OAuth OAuth 要求外部身份提供商使用 oAuth2 对客户端进行身份验证并发出访问令牌。当客户端将此令牌作为 API 网关的访问凭据提供时，该令牌将根据配置的值进行验证。

- **JWKS URI** -具有用于智威汤逊（JSON Web 令牌）验证的 JWT（JSON Web 密钥）的端点的 URL
- 颁发 者-身份验证服务器的身份（通常是 URL）。
- 受众 -令牌适用的服务或应用程序的标识。
- 要保存的声 明-访问权限表示为一组声明和预期值。以 CSV 格式指定声明值。
- 内省 **URI** -身份验证服务器的内省端点 URL。此 URL 用于验证不透明的访问令牌。有关这些令牌的更多信息，请参阅不透明访问令牌的 OAuth 配置。

  指定 **Introspect URI** 后，指定 客户端 **ID** 和客户 端密 码以访问身份验证服务器。
- 允许的算法 -此选项允许您限制传入令牌中的某些算法。默认情况下，允许使用所有支持的方法。但是，您可以检查所选流量的所需算法。

成功验证后，API 安全性会授予对客户端的访问权限。

> 重要：
>
> 在为选定的 API 资源配置 OAuth 或 **Auth-Basic** 策略时，请为其余 API 资源配置“无身份验证”策略。此配置明确表示您希望跳过其余资源的身份验证。

Authorization（授权） 此策略验证访问 API 资源所需的权限。访问权限表示为一组声明和预期值。要配置此策略，请选择 添加新声 明并指定以下内容：

- 索赔名称
- 索赔价值

> 重要：
>
> API 安全性需要针对 API 流量的身份验证和授权策略。因此，您必须使用身份验证策略配置授权策略。身份验证策略可以是 OAuth 或 `Auth-Basic`。
>
> 即使您没有任何授权检查，也必须使用空声明创建授权策略。否则，请求会因 403 错误而被拒绝。

速率限制

指定给所选 API 资源的最大负载。使用此策略，您可以监视 API 流量速率并采取预防措施。要配置此策略，请指定以下内容：

- **HTTP** 标头名称 -这是一个流量选择器密钥，用于过滤流量以识别 API 请求。此外，利率限制策略仅适用于此类 API 请求并进行监视。
- 标头值 -对于上述标头名称，这些标头值用逗号分隔。
- 阈值 -在指定时间间隔内可以允许的最大请求数。如果您指定了 标头值，则此阈值适用于每个标头值。

  示例 **1**：

当您为标头名称 `x-api-key` 指定标头值 (`"key1","key2","key3"`) 并将阈值设置为 80 时，设置的阈值适用于每个标头值。

示例 **2**：

如果要为每个标头值指定不同的阈值，请使用相同的 HTTP 标头名称创建单独的速率限制策略。

- **Policy-1**：为标头名称 `x-api-key` 指定标头值 (`"key1","key2"`)，并将阈值设置为 80。
- **Policy-2**：为标头名称 `x-api-key` 指定标头值 (`"key3"`)，并将阈值设置为 30。

如果您未指定标头值，则阈值适用于指定的 HTTP 标头名称。

- 时间片 -以微秒为单位指定的间隔。在此时间间隔内，请求将根据配置的限制进行监视。默认情况下，它设置为 1000 微秒（1 毫秒）。
- 限制类型 -您希望如何应用费率限制策略的模式。您可以选择 突发 或 平滑 限制类型。
- 操作 -定义要对超出阈值的流量采取的操作。您可以指定以下操作之一：
  - **DROP**：将请求删除超过配置的流量限制。
  - **RESET**：重置请求的连接。
  - 重定向：将流量重定向到已配置的 redirect_url。
  - 响应：使用标准响应 (`429 Too many requests`) 进行响应。

WAF

此政策可防止安全漏洞、数据丢失以及可能对访问敏感业务或客户信息的网站进行未经授权的修改。

在配置 WAF 策略之前，请使用样书在 NetScaler 控制台中创建 WAF 配置文件。

在 **WAF** 配置文件名称中，选择或指定您创建的 WAF 配置文件。

机器人

此策略可识别坏机器人并保护您的设备免受高级安全攻击。

在配置 BOT 策略之前，请使用样书在 NetScaler 控制台中创建机器人配置文件。

在 机器人配置文件名称中，指定您创建的机器人配置文件。

标题重写

此策略可帮助您修改 API 请求和响应的标题。如果要替换 HTTP 标头中的值，请指定以下内容：

- **HTTP** 标头名称：要在请求标头中修改的已提交的名称。

  示例：`Host`

- 标题值：可选，要在指定标头名称中修改的值字符串。

  示例：`sample.com`

- 标题新值：替换指定标题值的新值。

  如果未指定标头值，它会将任何接收的值替换为 **HTTP** 标头名称的指定值。

  示例：`example.com`

在此示例中，标头重写策略在 API 请求的 `Host` 字段中将 `sample.com` 替换 `example.com`。

URI 路径重写

此策略可帮助您修改 API 请求和响应的 URI 路径。如果要替换 URI 路径中的分段，请添加一条规则以执行以下操作之一：

- 替换路径段 -选择此操作类型时，请指定以下内容：

  - 当前路径段 -要替换的路径段。
  - 新路径分段 -仅替换当前路径段的新路径段。

  例如，要将 URI 路径中的区域设置从英语更改为中文，请在 当前路径段中指定 `/en-us/`。并且，在“新路径段”中指定 `/zh-zh`。它仅替换路径段并保留剩余的 URI 路径。

- 替换完整路径 -此操作类型将 API 请求和响应的 URI 路径完全替换为指定路径。如果您在“新路径分段”中指定 `/example.html`，则 API 请求或响应的 URI 路径将更改为指定路径。

- 移除路径分段 -此操作将从 URI 中删除指定分段。例如，要从 URI 路径中删除英语语言环境，请在当前路径段中指定 `/en-us/`。

- 插入路径分段 -此操作将指定段插入到 URI 路径中。要应用此规则，请指定要插入分段的位置。而且，您想插入哪个区段。

  例如，当您想在某个文本后面插入一个段落时，请执行以下操作：

  1. 指定要插入新分段的位置。
  2. 在“当前路径段”中，指定要在其后添加新段的文本。
  3. 在“新路径分段”中，指定要添加的分段。

拒绝

此策略可帮助您拒绝 API 请求访问您的 API 资源。

查看 **API** 分析

January 29, 2024

API 分析支持对 API 流量的可见性。这种分析使 IT 管理员能够监视 API 网关提供服务的 API 实例和端点。它提供对 API 请求的集成定期监视。

在监视 API 分析之前，请务必完成以下操作：

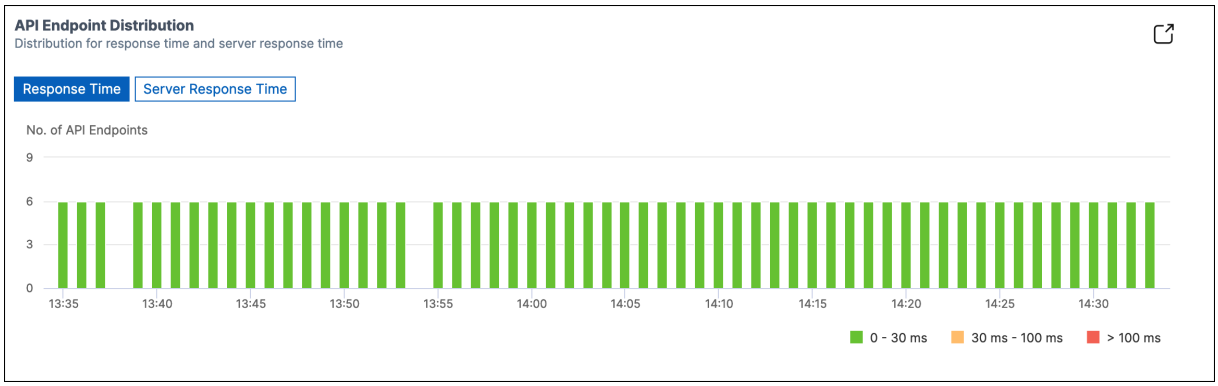
1. 添加 API 定义
2. 部署 API 定义
3. 向 API 定义添加策略
4. 向 API 实例申请许可证
5. 在 API 实例上启用 Web Insight

在 **API Analytics** 中，您可以监视作为 API 定义的一部分添加的 API 实例和端点的响应时间。它还显示 API 实例和终端节点消耗的带宽。

默认情况下，控制板显示最近一小时的 API 分析。您可以选择持续时间以查看该时间间隔的 API 分析。单击每个磁贴上的“查 看更多”以查看整个列表。在此视图中，您可以按除地理 位置 磁贴以外的部分名称搜索 API 实例和端点。

API 端点分发

此图显示了 API 端点的应用程序和服务器响应时间的分布。您可以识别响应时间长的 API 端点并采取必要的措施。



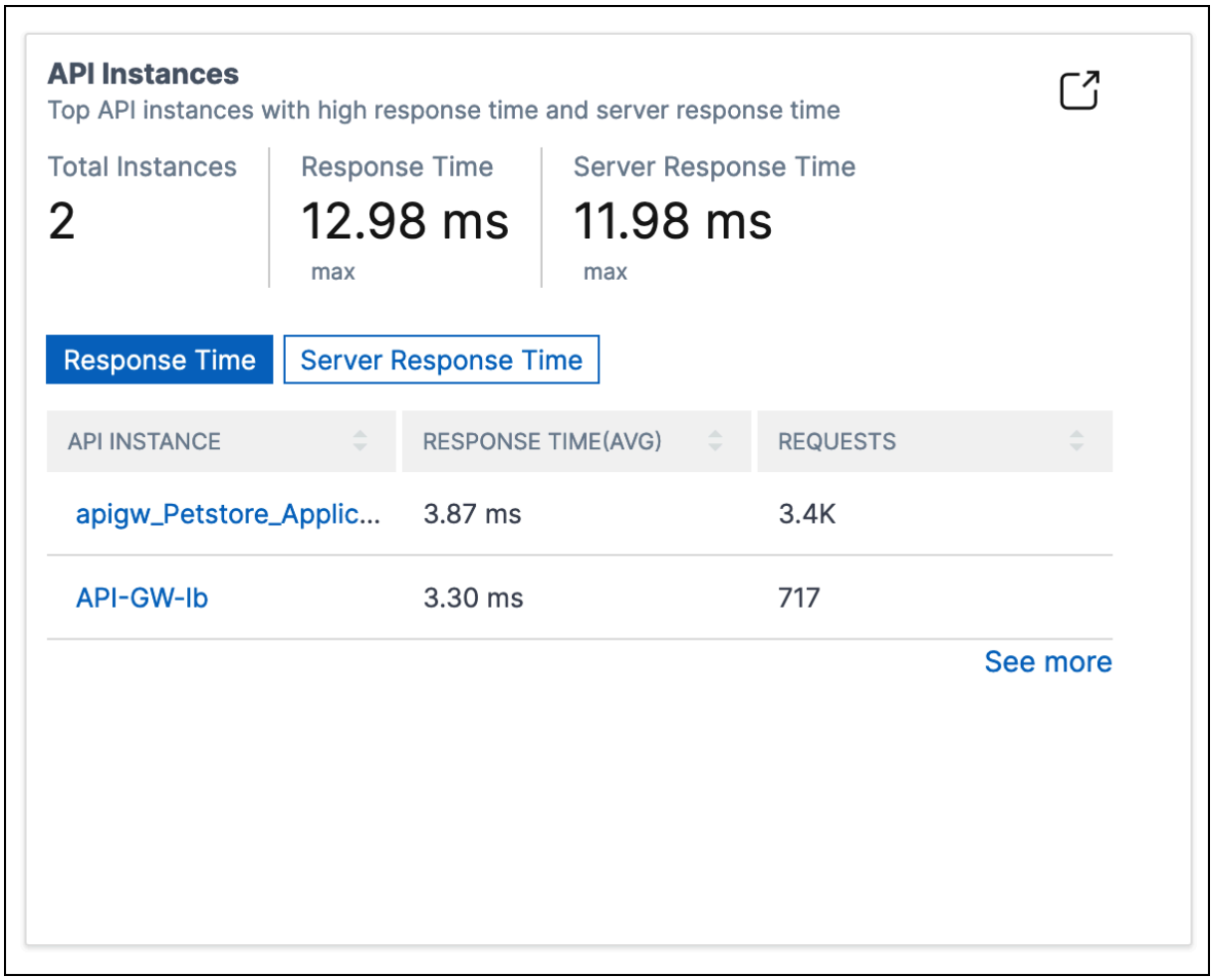
API 端点根据其响应时间限制以以下颜色之一显示：

- 绿色 -如果响应时间小于 30 毫秒。

- 橙色—如果响应时间介于 30—100 毫秒之间。
- 红色 -如果响应时间超过 100 毫秒。

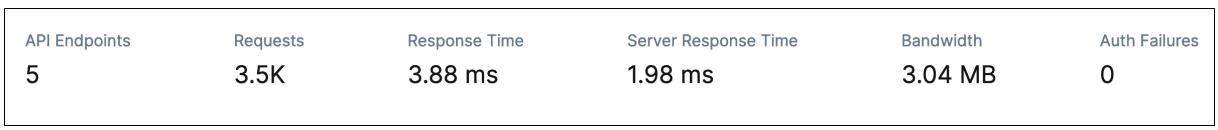
API 实例

API 实例 图块显示应用程序和服务器响应时间较长的顶级 API 实例。



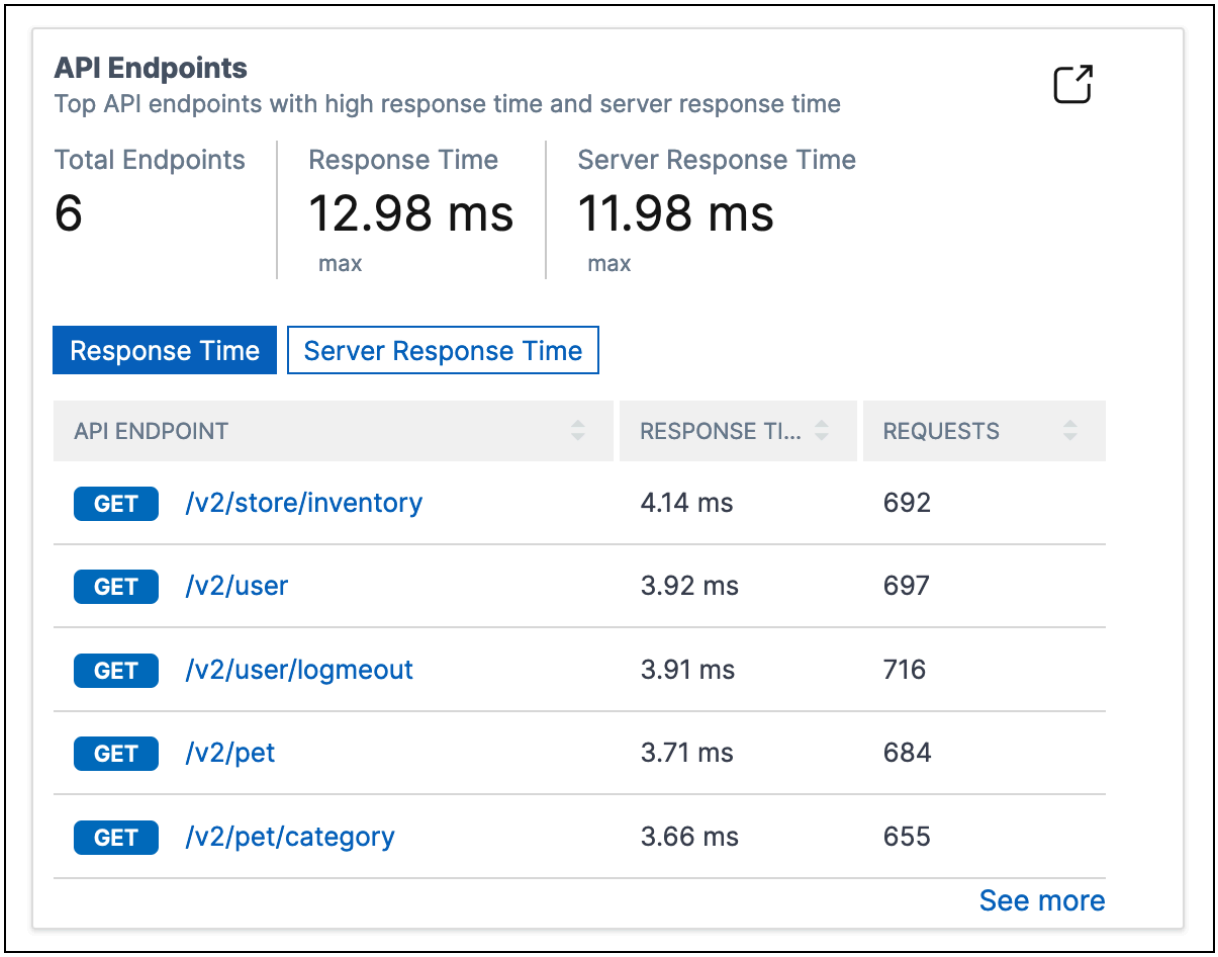
选择 API 实例以查看其性能、使用情况和安全详细信息。选定的 API 实例显示以下信息：

- API 端点数量
- 请求数
- 应用程序和服务器响应时间
- 消耗的带宽
- 身份验证失败



API 端点

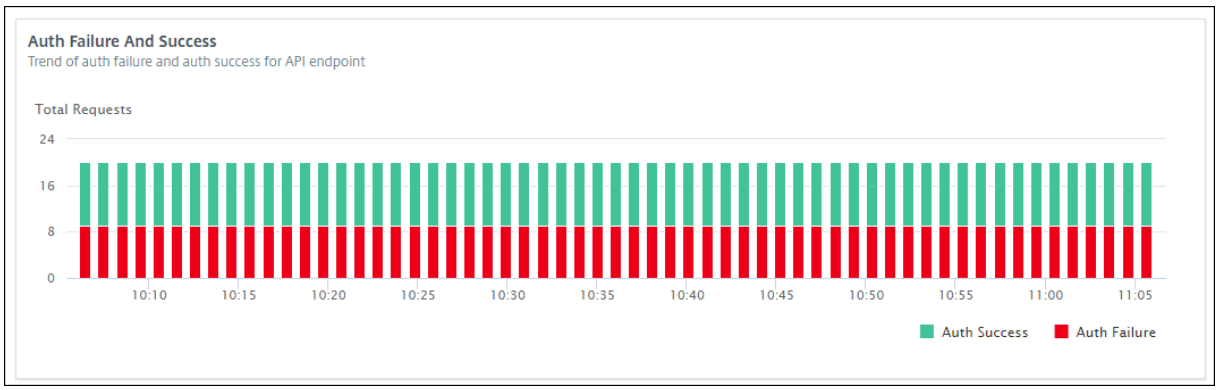
API 端点图标显示应用程序和服务器响应时间较长的顶级端点。



选择 API 端点以查看性能、使用情况和安全详细信息。

身份验证失败

身份 验证失败 图块显示身份验证失败次数较多的顶级 API 端点。身份验证失败或成功是根据添加到 API 定义中的策略发生的。



如果要查看 API 端点中的身份验证失败和成功率，请执行以下操作：

1. 从 **API** 端点中选择一个端点。
2. 选择安全选项卡。此选项卡显示所选端点中的身份验证失败和成功情况。

如果您想查看实例的 API 端点中的身份验证失败和成功率，请执行以下操作：

1. 从 **API** 实例中选择一个实例。
2. 选择安全选项卡。此选项卡显示所选实例的端点中的身份验证失败和成功情况。

查看不同的 **API** 见解

在 API Analytics 中导航以查看有关以下内容的特定信息：

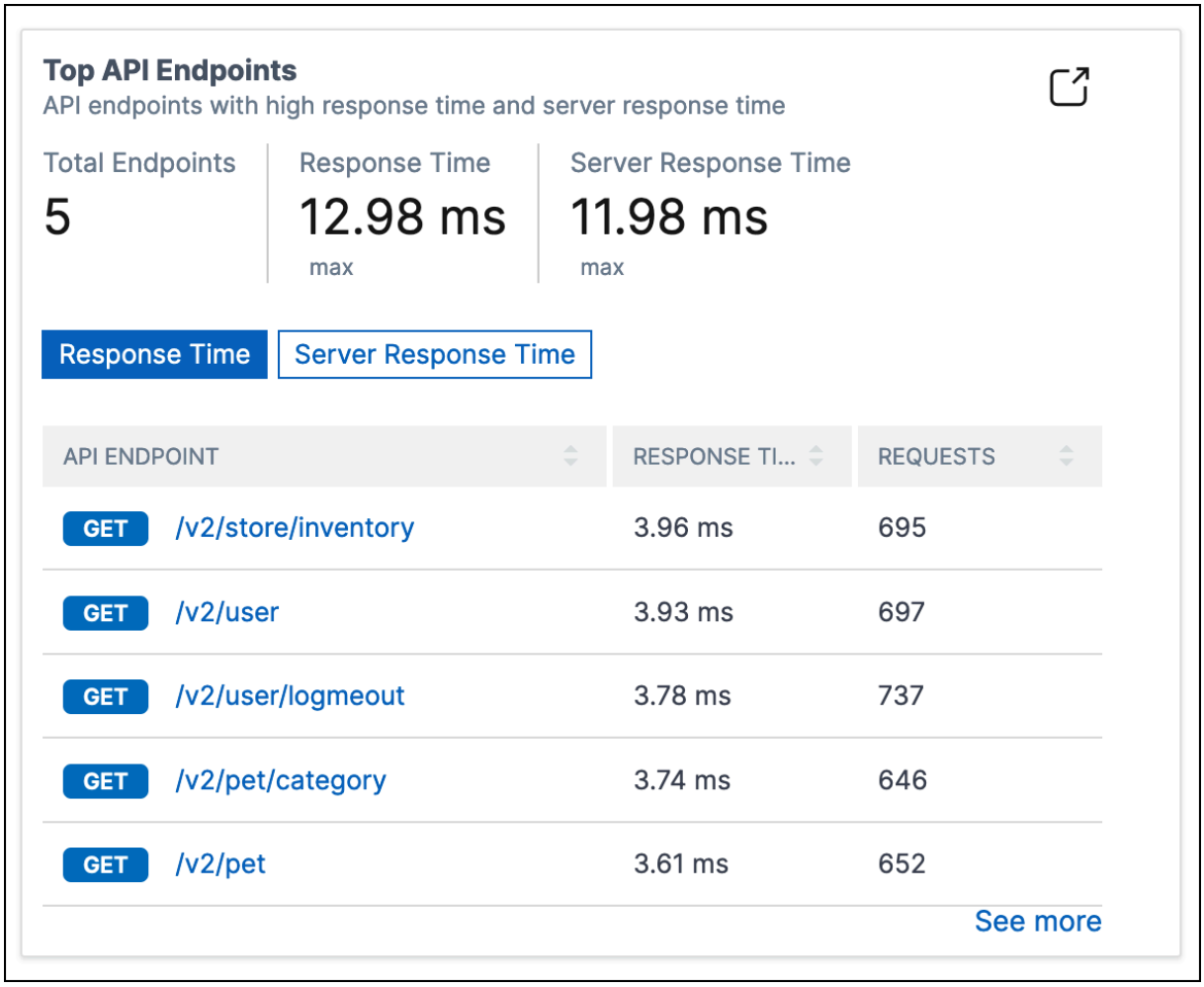
- 实例中的最多 API 端点
- 访问次数最多的 API
- 端点的地理位置

- HTTPS 响应状态
- API 请求趋势
- 端点的带宽消耗
- SSL 错误和使用情况

查看实例中的主要 **API** 端点

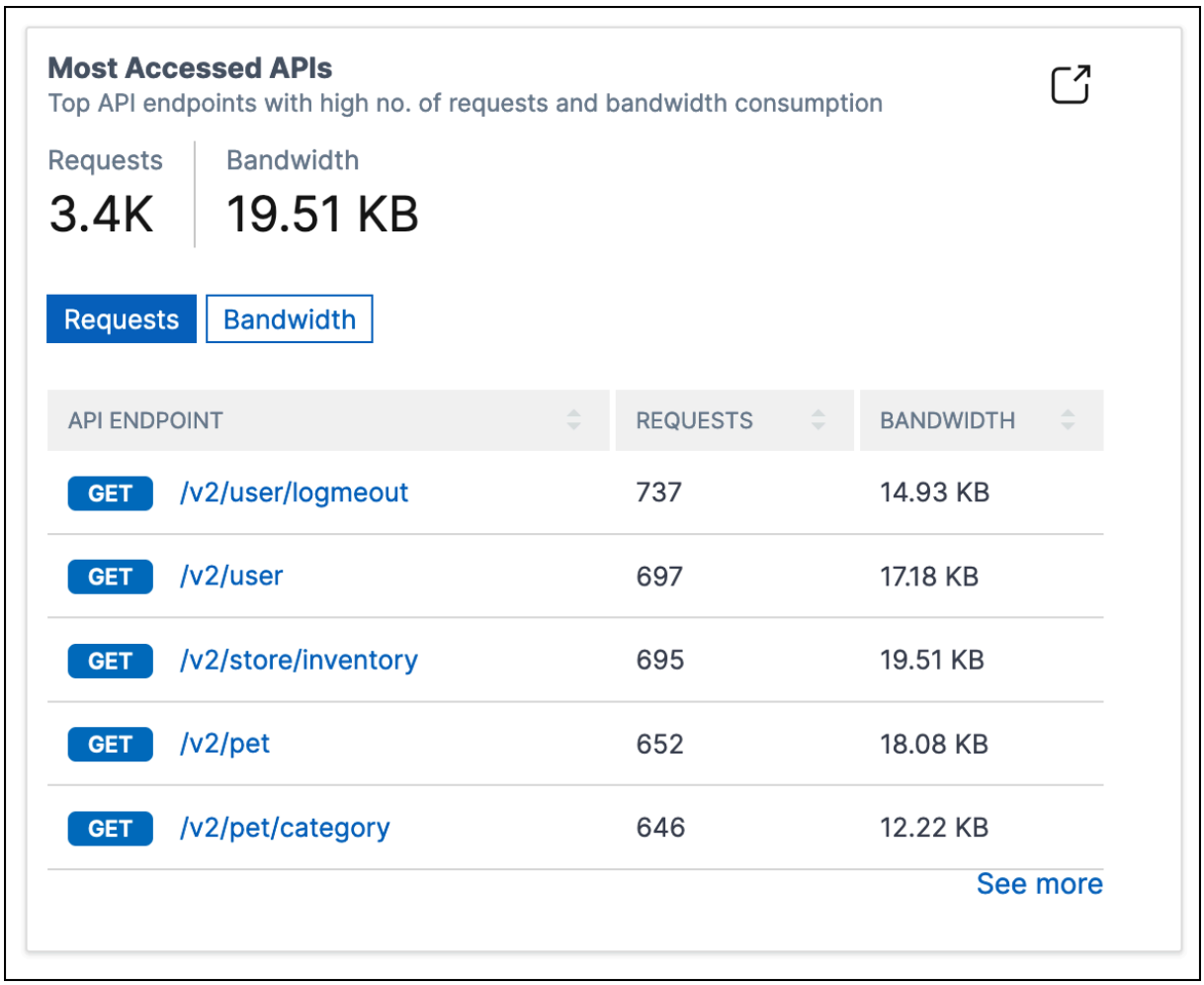
API Analytics 页面显示响应时间较长的顶级端点。如果您想查看实例的相似端点，请从 **API** 实例中选择一个实例。

“最 佳 **API** 端点”图标显示应用程序和服务器响应时间较长的端点。



查看访问次数最多的 **API**

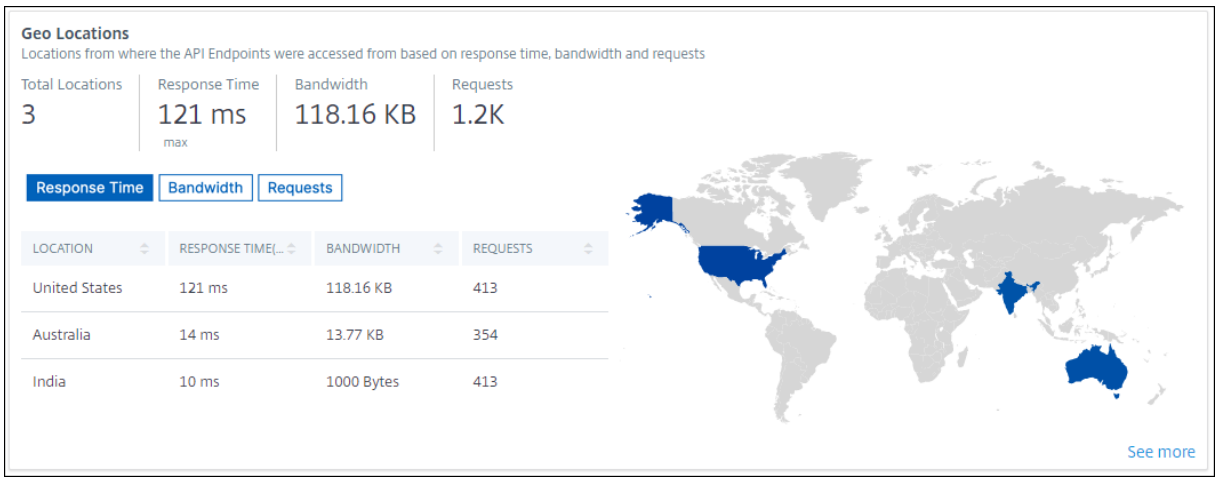
在 **API** 分析中，从 API 实例中选择一个 API 实例。“访问次数最多 **API**”图块显示了具有更多请求和带宽的顶级端点。



查看端点的地理位置

1. 在 **API** 分析中，选择以下任意选项：
   - 从 **API** 实例 中选择一个实例，查看所选实例的端点接收请求的位置。
   - 从 **API Endpoints** 中选择一个端 点以查看该端点接收请求的位置。
2. 在“性能和使用情况”中，将出现“地理位置”图块。

   您可以根据响应时间、带宽和请求对位置进行排序。

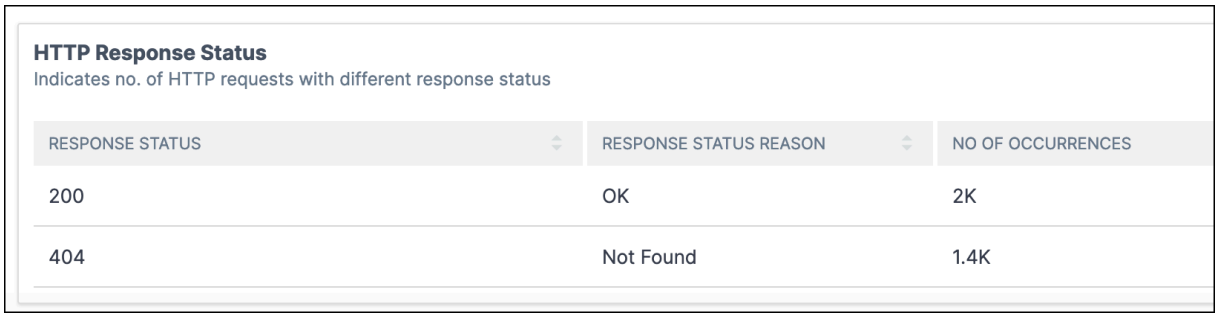


查看 **HTTPS** 响应状态

HTTPS 响应状态图块显示响应状态及其原因和发生次数。您可以通过以下方式之一查看 HTTPS 响应状态：

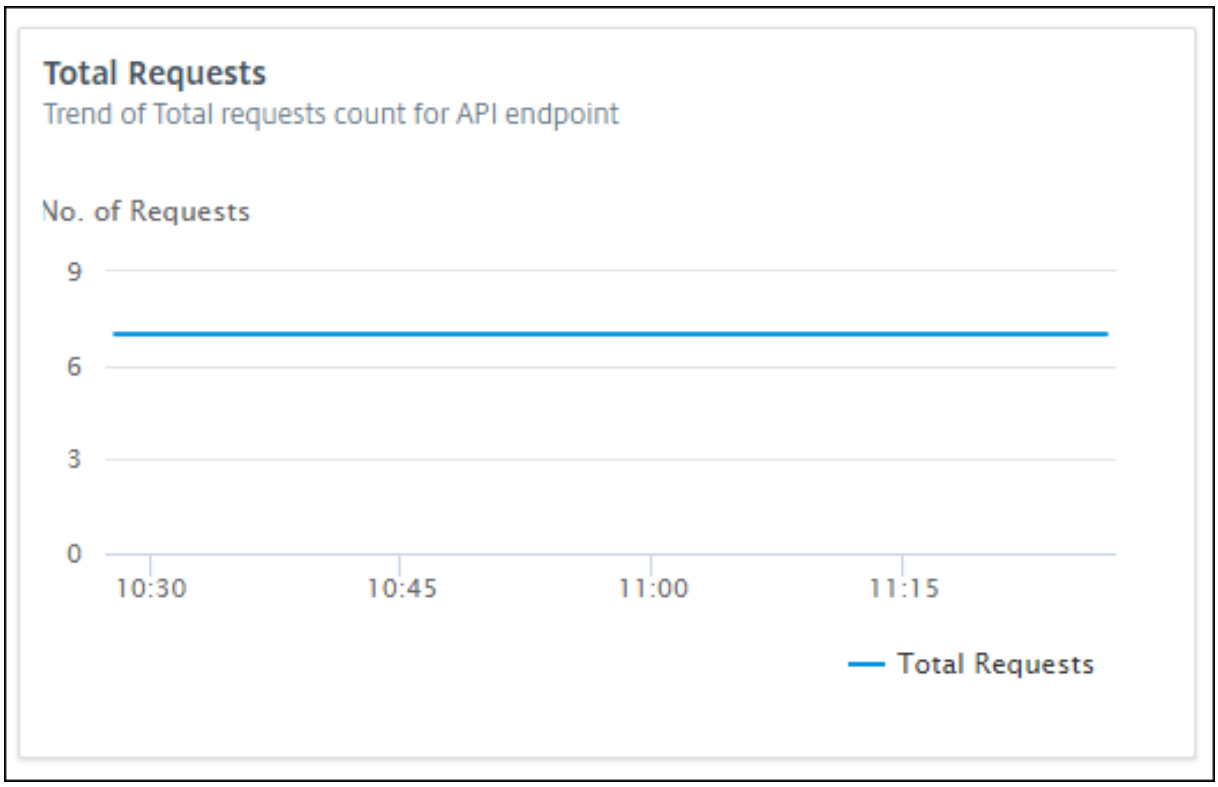
- 从 **API** 实例中选择一个实例。
- 从 **API** 端点中选择一个端点。

此磁贴显示在“性能和使用情况”选项卡中。

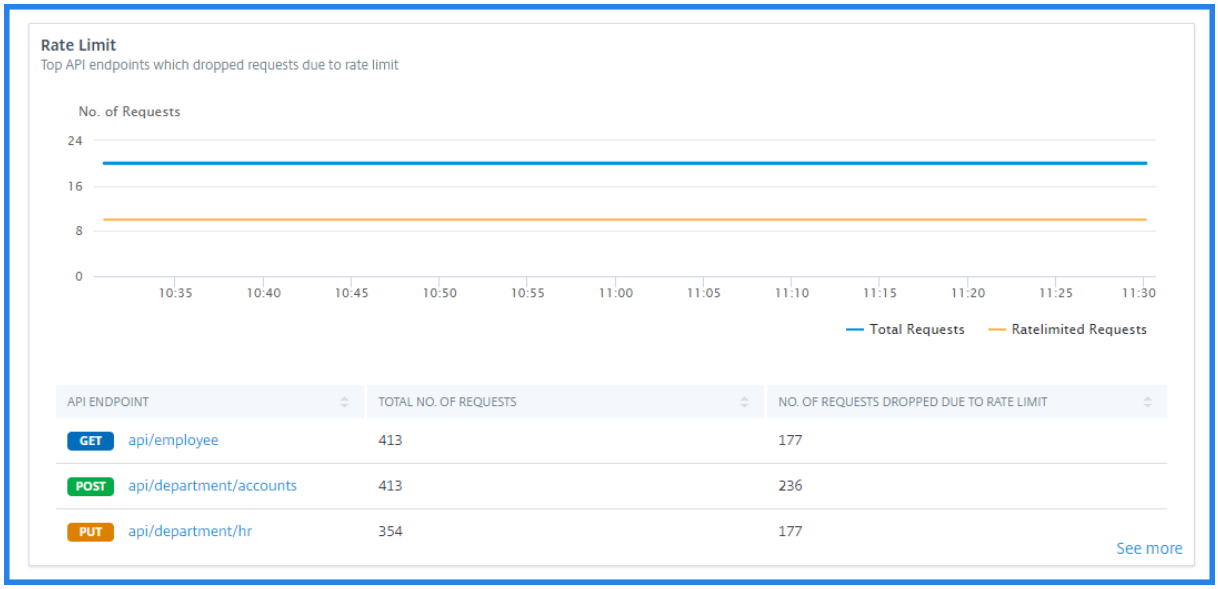


查看 **API** 请求趋势

从 **API** 端点中选择一个端点。在“性能和使用情况”中，“请求总 数”图块显示端点收到的请求总数的趋势。



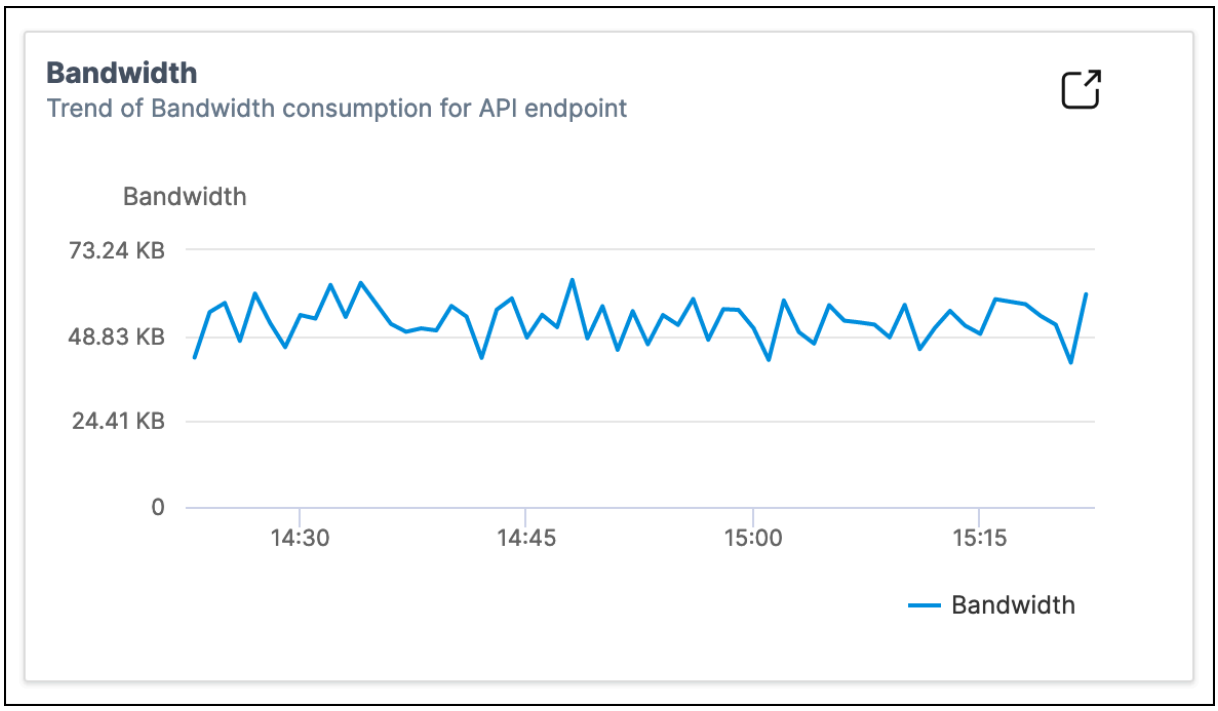
如果您想查看由于速率限制而丢弃请求的趋势，请从 **API** 实例中选择一个实例。在“安全”中，速率限制 图块显示请求丢弃的趋势。它还显示端点收到的请求总数的趋势。



通过这种比较，您可以确定由于总请求的速率限制而丢弃了多少请求。

查看端点的带宽消耗

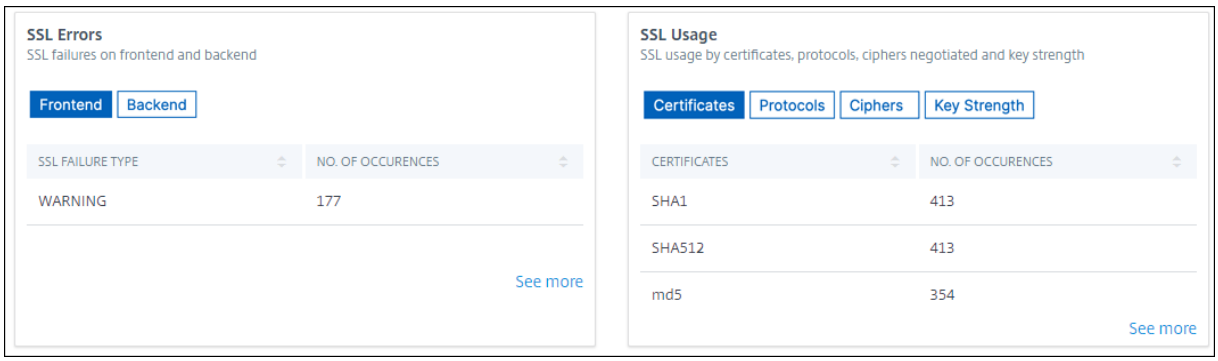
要查看端点的带宽消耗趋势，请从 API 端点中选择一个端点。带宽 图块显示带宽消耗图表。



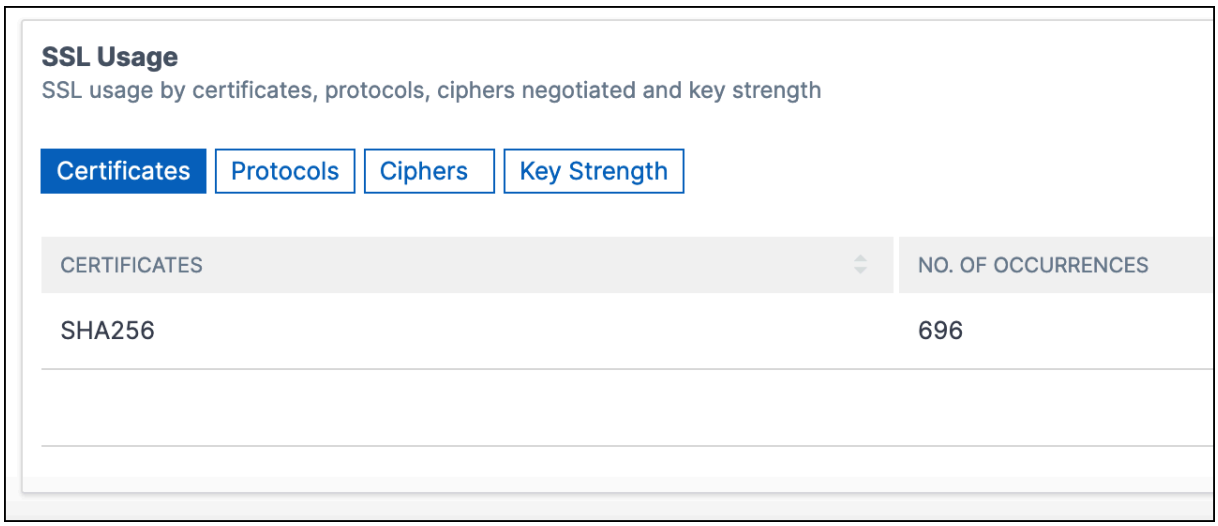
查看 **SSL** 错误和使用情况

从 **API** 实例中选择一个实例。在“安全”中，将显示以下图块：

- **SSL** 错误 -显示客户端和应用程序服务器上发生的 SSL 故障。
- **SSL** 使用情况 - 显示 SSL 证书、协议、密码及其出现的密钥强度。



要查看端点中的 SSL 使用情况，请从 API 端点中选择一个端点。**SSL** 使用情况 图标显示在“安全”选项卡中。



发现 **API** 端点

July 17, 2024

您可以使用 API 安全性查看在您的组织中发现的 API 终端节点。NetScaler 控制台根据在 NetScaler 实例和 API 部署上收到的 API 流量发现 API 端点。

在 NetScaler 控制台中，安全 **> API** 安全 **> API** 发现页面显示发现的 API 端点。

- 虚拟服务器 - 虚拟服务器选项卡显示来自您的 NetScaler 实例的虚拟服务器。虚拟服务器在指定时间段内收到 API 请求时，它们将显示在此选项卡中。
- **API** 部署 - 此选项卡显示使用 API 定义从 NetScaler 控制台部署的 API 部署。此选项卡将在 API 部署在指定期间内收到 API 请求时发现 API 端点。要添加和部署 API 定义，请参阅添加 API 定义和部署 API 定义。

> 注意：
>
> - 确保在虚拟服务器上配置分析并启用 Web Insights。请参阅在 API 实例上启用 Web Insight。
> - 您只能将策略添加到 **API** 部署选项卡下发现的 API 端点。

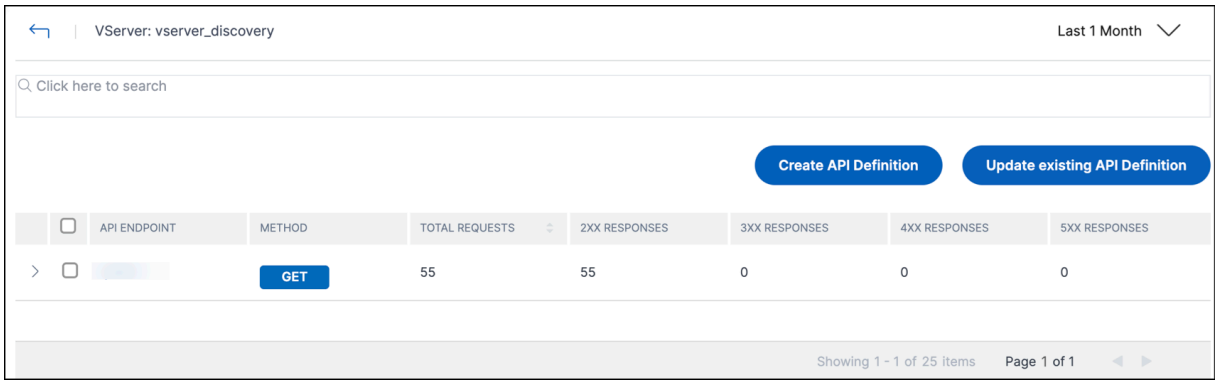
查看 **API** 端点

在 **API** 发现中，当您选择虚拟服务器或 API 部署时，NetScaler 控制台 GUI 会显示 API 端点及其详细信息，例如：

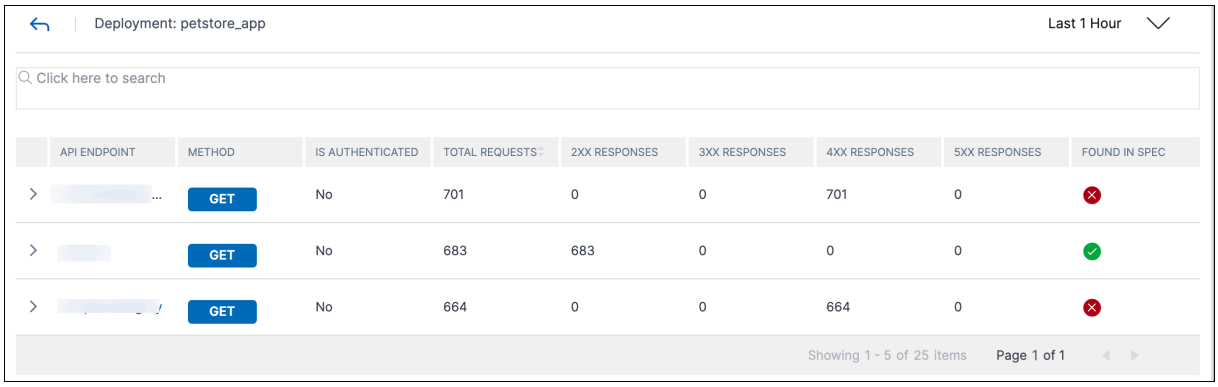
- 方法 -它显示 API 端点中使用的方法。例如，GET 和 POST 方法。
- 请求总数 - 它显示 API 端点上的 API 请求计数。
- 响应状态 -它显示每个响应状态的计数。例如，2xx、3xx、4xx 和 5xx。

- 在规范中找到 -此列仅适用于 API 部署。有时，不属于 API 定义的内部 API 可能会接收来自外部的流量。此列可帮助您确定 API 端点和观察方法是否属于 API 定义的一部分。

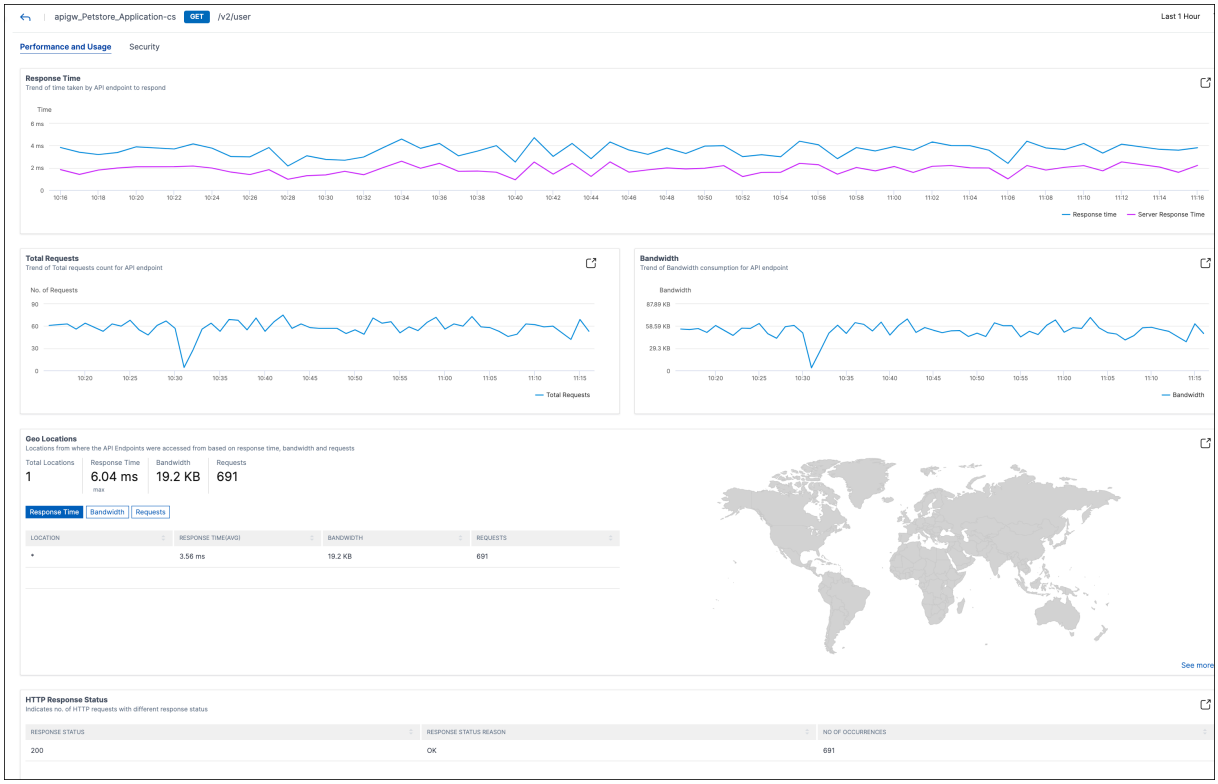
虚拟服务器中的 API 端点可用如下：



API 部署中的 API 端点可用如下：



您还可以选择所需的 API 端点以查看其详细的分析报告。

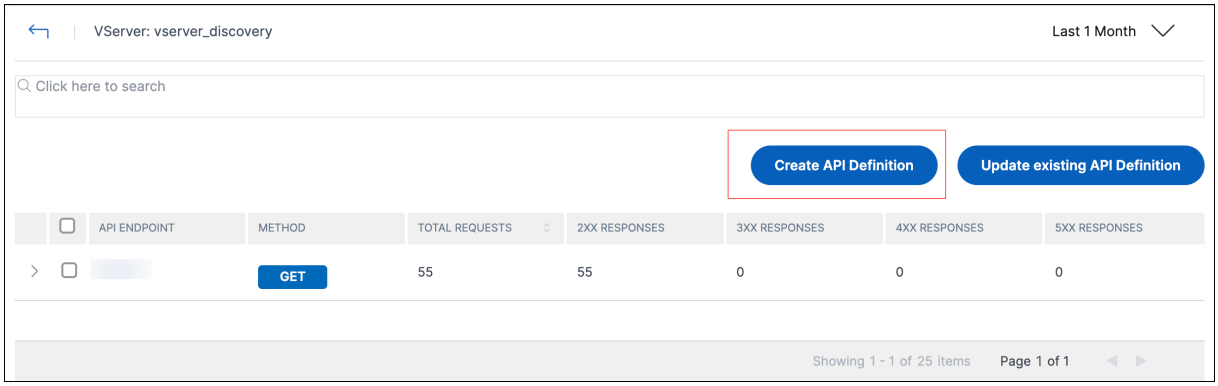


有关每个部分的更多信息，请参阅 查看 API 分析。

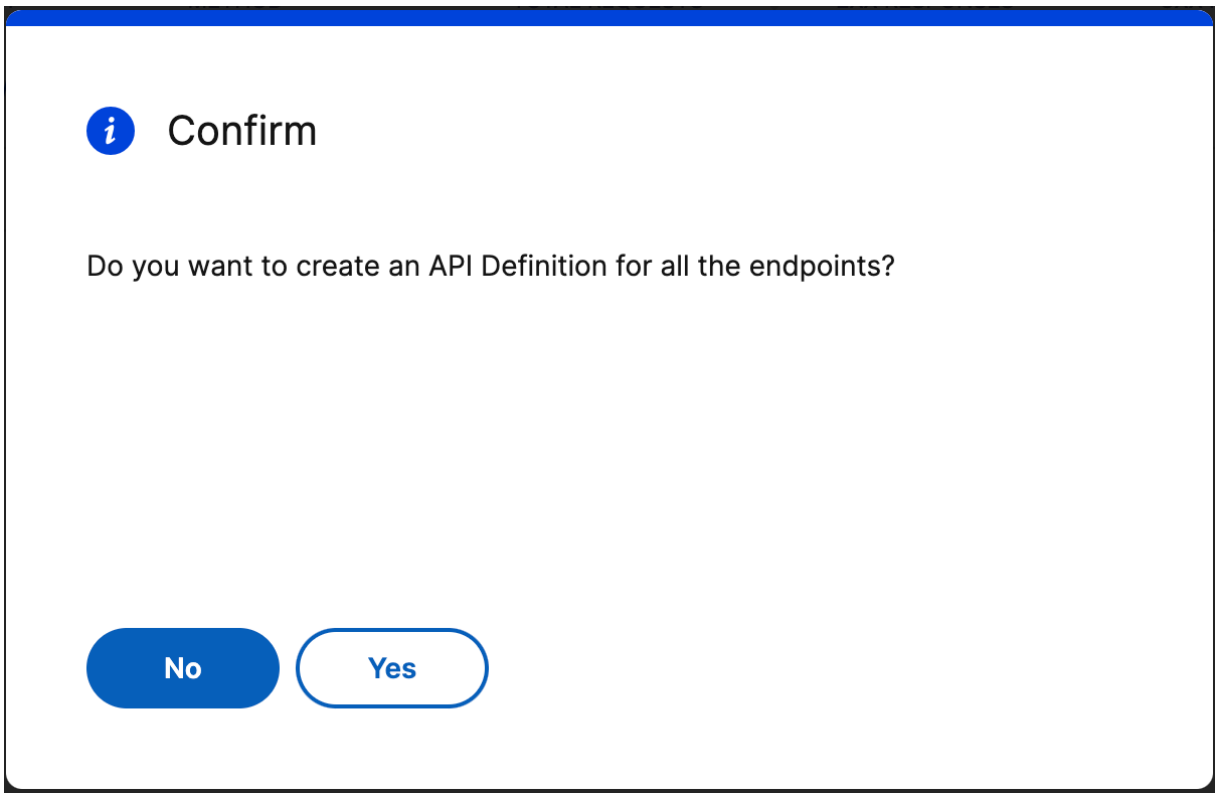
从发现的 **API** 端点创建 **API** 定义

要从发现的 API 端点（API 资源和方法）创建 API 定义，请执行以下操作：

1. 导航到安全性 **> API** 安全性 **> API** 发现，查看虚拟服务器和 API 部署列表。
2. 在“虚拟服务器”选项卡中单击任意虚拟服务器。
3. 虚拟服务器页面显示已发现的端点列表。选择任意端点，然后单击“创建 **API** 定义”。

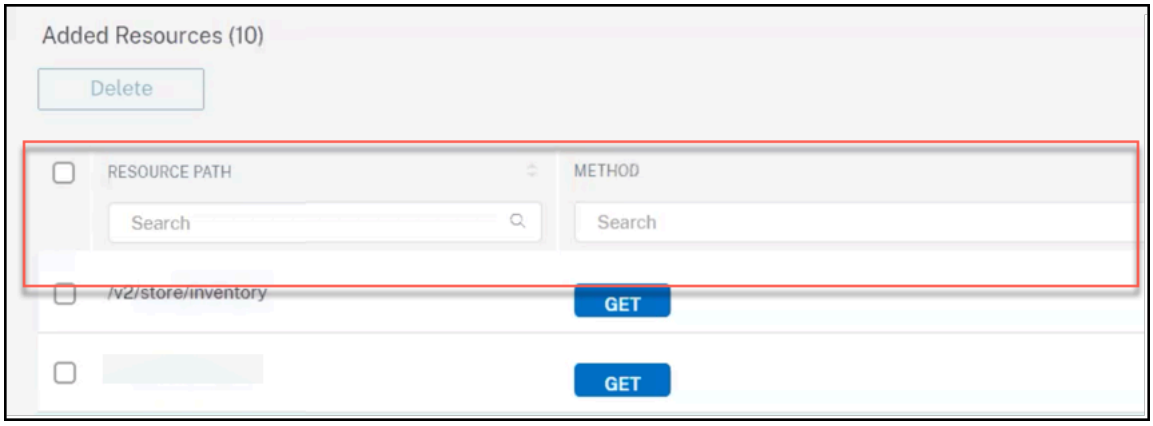


> 注意：
>
> 如果您未选择任何端点并单击“创建 **API** 定义”，则会出现一个弹出窗口，供您确认是否要为所有端点创建 API 定义。单击“是”以创建包含所有端点的 API 定义，否则单击“否”。



1. 在 创建 **API** 定义中，指定以下内容：
   - 名称 -API 定义的名称。
   - **API** 定义 -定义必须包括标题、版本、基本路径和主机。您可以在 主 机字段中指定域名或 IP 地址。
   - **API** 资源 -向定义中添加多个 API 资源。每个资源都有一个路径和支持的方法。
2. 单击“创建定义”创建 API 定义。

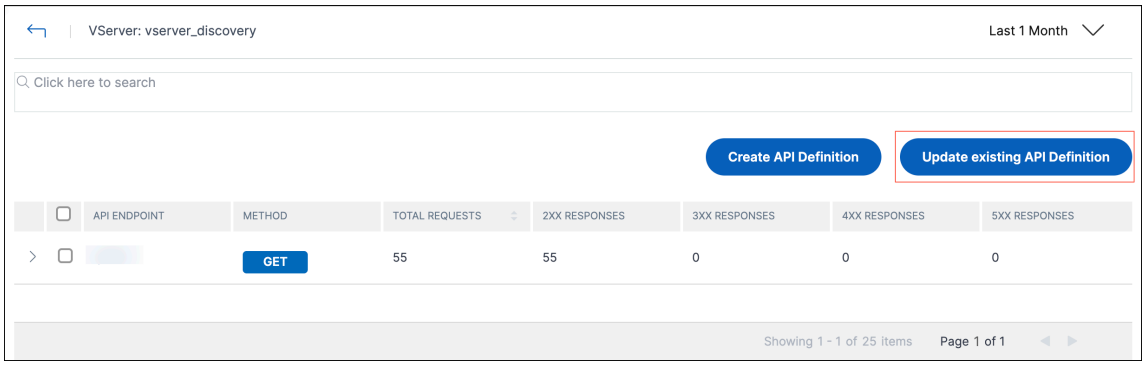
> 注意：
>
> 如果要在将 API 资源路径添加到 API 定义之前对其进行编辑，请在 API 定义屏幕上使用 API 资源的排序或搜索功能。
>
> 例如，假设一个名为“/api/products/123-3243-2344334/reviews”的 API 资源，其中路径段“123-3243-2344334”是一个可变的产品 ID。您现在可以对 API 资源进行排序，将资源路径添加为“/api/products/{id}/reviews”，并删除所有 ID 为“/api/products/123-3243-2344334/reviews”的 API 终端节点。



使用发现的 **API** 端点更新现有 **API** 定义

要使用 API 端点（API 资源和方法）更新现有 API 定义，请执行以下操作：

1. 导航到安全性 **> API** 安全性 **> API** 发现，查看虚拟服务器和 API 部署列表。
2. 在“虚拟服务器”选项卡中单击任意虚拟服务器。
3. 虚拟服务器页面显示已发现的端点列表。选择要添加到现有 API 定义的终端节点。单击“更新现有 **API** 定义”。



4. 从“选择现有 **API** 定义”下拉列表中，选择要更新的 API 定义。单击“更新定义”。
5. 将出现“更新现有 **API** 定义”页面。**API** 资源 部分显示以下表格：
   - 已添加资源 -您选择的 API 端点
   - 现有资源 -API 定义中已提供的 API 端点

   > 注意：
   >
   > 如果在“已添加的资源”和“现有资源 **”中存在相同的 API 端点，则该端点只会添加一次 API 定义中。

6. 单击“更新定义”。

取消部署 **API** 实例

January 29, 2024

当您想要从 NetScaler 实例中删除 API 实例配置时，可以使用“取消部署”选项，但将 API 实例对象作为草稿保留在 NetScaler 控制台中。此操作将“部署状态”设置为“草稿中”。而且，它只能应用于已部署的 API 实例配置。

> 重要：
>
> - 在取消部署 API 部署之前，请确保所有关联的 API 策略均已取消部署或删除。请参阅取消部署 API 策略。
> - 在取消部署 API 代理之前，请确保所有关联的 API 部署均已卸载或删除。请参阅，取消部署 API 部署。

取消部署 **API** 策略

按照以下步骤取消部署 API 策略：

1. 在“安全”**>**“**API** 安全性”**>**“策略”中，选择要取消部署的策略。
2. 单击“取消部署”。

此操作将“策略状态”设置为“草稿中”。

取消部署 **API** 部署

按照以下步骤取消部署 API：

1. 在安全性 **> API** 安全性 **> API** 部署中，选择要取消部署的 API 部署。

   > 注意：
   >
   > 确保已取消部署或删除所选部署的所有关联策略。

2. 单击“取消部署”。

此操作将“部署状态”设置为“草稿中”。

取消部署 **API** 代理

按照以下步骤取消部署 API 代理：

1. 在“安全性”**>**“**API** 安全性”**>**“**API** 代理”中，选择要取消部署的 API 代理。

> 注意：
>
> 您可以与不同的 API 部署共享 API 代理。因此，请确保已卸载或删除所选代理的所有关联部署。

2. 单击“取消部署”。

此操作将“代理状态”设置为“草稿中”。

使用 **API** 来管理 **API** 安全性

January 29, 2024

您可以访问 API 来创建、配置和部署 API 安全性。

> 注意：
>
> 要了解如何使用 API 安全性 API 来配置该功能，请参阅 Nitro API 文档。

	步骤	资源 URL
1	创建 API 定义	`https://adm.cloud.com/{ customerid } /apisec/nitro/v1/config/apidefs`
2	添加 API 代理	`https://adm.cloud.com/apiproxies`
3	使用 API 代理部署 API 实例	`https://adm.cloud.com/apiproxies/{ customerid } /deployments`
4	添加 API 策略	`https://adm.cloud.com/{ customerid } /apisec/nitro/v1/config/policies/{ id }`

每个 API 策略都有不同的 `config_spec` 对象。它是一个不透明的对象，它包含一个 JSON 字典，用于使用特定值配置 `policytype`。

在此对象中，您可以使用以下选项选择 API 资源及其方法：

- `api-resource-paths` - 指定 API 定义中定义的 API 资源路径和方法。

  示例：

```
{

"endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags"],
    "get": true,
    "post": false,
    "put": false,
    "delete": false
 }
```

- `custom-rules` - 指定 API 定义中可能不存在的自定义 API 资源路径和方法。

  示例：

```
{

"endpoints": ["/pet/categories", "/pet/findByName"],
    "get": true,
    "post": false,
    "put": false,
    "delete": false
 }
```

使用此配置，策略会筛选与指定 API 资源路径匹配的传入流量请求。

有关每种策略类型的 `config_spec` 的信息，请参阅策略类型的 API 示例。

策略类型的 **API** 示例

本节介绍支持的 API 策略类型及其配置：

- 速率限制
- OAuth
- 基本认证
- 未进行身份验证
- 机器人
- WAF
- 标题重写
- URI 路径重写
- Authorization（授权）
- 拒绝

速率限制

以下是 `Ratelimit` 策略类型的示例配置。在 `config_spec` 对象中指定以下配置：

```
{

    "policytype": "Ratelimit",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "threshold": "10",
        "timeslice": "20000",
        "limittype": "BURSTY",
        "api-respondertype": "DROP",
        "header_name": "x-api-key",
        "per_client_ip": true
     }
 ,
    "order_index": 1,
    "policy_name": "ratelimit_policy"
 }
```

有关每个属性的更多信息，请参阅 速率限制策略。

OAuth

下面是 `JWT Auth validation` 策略类型的 API 配置示例。在 `config_spec` 对象中指定以下配置：

```
{

    "policytype": "JWT Auth Validation",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
```



```
            "put": false,
            "delete": false
         }
,
        "custom-rules": {
 }
,
        "jwks-uri": "https://uri.petstore.com",
        "issuer": "https://issuer.petstore.com",
        "audience": "petstore",
        "introspect-uri": "https://introspect.uri.com",
        "clientid": "client",
        "clientsecret": "clientsecret",
        "claims-to-save": ["scope", "scope2"],
        "allowed-algorithms": {

            "hs256": true,
            "rs256": true,
            "rs512": true
         }

     }
,
   "order_index": 2,
   "policy_name": "Jwt_auth_policy"
}
```

有关每个属性的更多信息，请参阅 OAuth 策略

基本认证

以下是 BasicAuth 策略类型的 API 配置示例：

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false
         }
,
        "custom-rules": {
 }

     }
,
```



```
    "order_index": 3,
    "policy_name": "Auth_BaSIC",
    "policytype": "BasicAuth"
 }
```

有关每个属性的更多信息，请参阅 基本身份验证策略。

未进行身份验证

以下是 NoAuth 策略类型的 API 配置示例：

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": false,
            "put": false
         }
 ,
        "custom-rules": {
  }

     }
 ,
    "order_index": 4,
    "policy_name": "no_auth_policy",
    "policytype": "NoAuth"
}
```

机器人

以下是 Bot 策略类型的 API 配置示例：

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": false,
            "post": false,
```



```
            "put": false
          }
  ,
        "bot-prof-name": "apisec_test_profile",
        "custom-rules": {
   }

     }
  ,
    "order_index": 5,
    "policy_name": "bot_policy",
    "policytype": "Bot"
  }
```

有关每个属性的更多信息，请参阅机器人策略。

WAF

以下是 WAF 策略类型的 API 配置示例：

```
{

    "config_spec": {

        "api-resource-paths": {

            "delete": false,
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": false,
            "post": false,
            "put": false
          }
  ,
        "waf-prof-name": "apisec_waf_profile",
        "custom-rules": {
   }

     }
  ,
    "order_index": 6,
    "policy_name": "waf_policy",
    "policytype": "WAF"
  }
```

有关每个属性的更多信息，请参阅 WAF 策略。

标题重写

以下是 Header Rewrite 策略类型的 API 配置示例，请在 `config_spec` 对象中指定此配置：


```
{

    "policytype": "Header Rewrite",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "rewrite-policy-header-field-name": "org",
        "rewrite-policy-header-field-val": "Citrix",
        "rewrite-policy-header-field-new-val": "Citrite"
     }
 ,
    "order_index": 7,
    "policy_name": "header_rewrite_pol"
 }
```

有关每个属性的更多信息，请参阅标题重写策略。

URI 路径重写

以下是 URI 路径重写策略类型的 API 配置示例：

```
{

    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/store/order", "/store/inventory"],
            "delete": false,
            "get": true,
            "post": true,
            "patch": false,
            "put": false
         }
 ,
        "custom-rules": {

            "delete": false,
            "endpoints": [],
```



```
            "get": false,
            "post": false,
            "patch": false,
            "put": true
         }
,
        "path-rewrite-params": [
        {

            "insert-segment-position": "beginning",
            "new-path-value": "v3",
            "old-path-value": "v2",
            "action-type": "replace path segment"
         }
,
        {

            "insert-segment-position": "beginning",
            "new-path-value": "begin",
            "action-type": "insert path segment"
         }
,
        {

            "insert-segment-position": "end",
            "new-path-value": "end",
            "action-type": "insert path segment"
         }
,
        {

            "insert-segment-position": "before",
            "new-path-value": "before",
            "old-path-value": "store",
            "action-type": "insert path segment"
         }
,
        {

            "insert-segment-position": "after",
            "new-path-value": "after",
            "old-path-value": "store",
            "action-type": "insert path segment"
         }

        ]
    }
,
        "order_index": 24,
        "policy_name": "eats_uripathrewrite",
        "policytype": "URI Path Rewrite”
}
```


有关每个属性的更多信息，请参阅 URI 路径重写策略。

Authorization（授权）

下面是 Authorization 策略类型的 API 配置示例。在 config_spec 对象中指定以下配置：

```
{

    "policytype": "Authorization",
    "config_spec": {

        "api-resource-paths": {

            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
         }
 ,
        "custom-rules": {
  }
 ,
        "claims": [{

            "name": "scope",
            "values": ["value1", "value2"]
         }
 ]
     }
 ,
    "order_index": 8,
    "policy_name": "authorization"
 }
```

有关每个属性的更多信息，请参阅授权策略。

拒绝

下面是 Deny 策略类型的 API 配置示例。在 config_spec 对象中指定以下配置：

```
{

    "policytype": "Deny",
    "config_spec": {

        "api-resource-paths": {

```



```
            "endpoints": ["/pet", "/pet/findByStatus", "/pet/findByTags
                "],
            "get": true,
            "post": true,
            "put": false,
            "delete": false
          }
,
        "custom-rules": {
 }
,
        "api-denytype": "RESPONDWITH"
     }
,
   "order_index": 9,
   "policy_name": "deny_policy"
}
```

在 `api-denytype` 中，您可以指定以下值之一：

- RESPONDWITH
- RESET

有关每个属性的更多信息，请参阅 拒绝规则。

使用样书创建 **WAF** 和 **BOT** 配置文件

January 29, 2024

当您可以在 API **Gateway** 中为 API 资源选择策略时，它允许您定义流量选择标准来验证 API 请求。此外，它还允许您为 API 流量配置 API 安全性策略。有关更多信息，请参阅 API 安全。

您可以将 WAF 和 BOT 策略配置为 API 资源。在配置策略之前，请确保在 NetScaler 控制台中创建其配置文件。使用以下默认样书创建配置文件：

- API WAF 检测样书
- API BOT 检测样书

使用样书创建 **WAF** 配置文件

执行以下操作以创建 WAF 配置文件：

1. 在 NetScaler 控制台中，导航到应用程序 > 配置 > 样书。通过键入名称 `api-waf-profile` 搜索样书。单击 创建配置。

   样书将以用户界面页面形式打开，您可以在此为此样书中定义的所有参数输入值。

2. 为以下参数指定值：
    - **API WAF** 配置文件名称 -用于标识 WAF 配置文件的名称。
    - 应用程序类型 -向配置文件添加应用程序类型 WAF 配置文件支持 JSON 和 XML 应用程序类型。
3. 可选，启用 安全设置 以指定 HTTP、JSON 或 XML 保护检查。您还可以指定 NetScaler Web App Firewall 的错误 URL。有关详细信息，请参阅 创建 Web App Firewall 配置文件。
4. 选择要在其上部署此配置的目标 NetScaler 实例或实例组。
5. 单击创建。

要配置 WAF 策略，请参阅 将策略添加到 API 部署。

使用样书创建 **BOT** 配置文件

执行以下操作以创建 BOT 配置文件：

1. 在 NetScaler 控制台中，导航到应用程序 > 配置 > 样书。通过键入名称 `api-bot-profile` 搜索样书。单击 创建配置。

    样书将以用户界面页面形式打开，您可以在此为此样书中定义的所有参数输入值。
2. 在 **BOT** 配置文件名称中，指定用于标识 BOT 配置文件的名称。
3. 可选，根据您的要求启用以下选项：
    - 启用 **IP** 信誉检查 -此选项标识发送不需要请求的 IP 地址。您可以使用 IP 信誉列表来先发制人拒绝来自信誉不良的 IP 的请求。
    - 启用 **BOT** 签 名-指定 BOT 签名名称。它阻止来自指定签名的请求。
    - 允许列表 -指定 IPv4 或子网 (CIDR) 地址。此选项使 BOT 配置文件能够绕过来自指定 IPv4 或子网地址的请求。
    - 拒绝列表 -指定 IPv4 或子网 (CIDR) 地址。此选项使 BOT 配置文件能够阻止来自指定 IPv4 或子网地址的请求。
4. 选择要在其上部署此配置的目标 NetScaler 实例或实例组。
5. 单击创建。

要配置 BOT 策略，请参阅 将策略添加到 API 部署。

应用程序

April 10, 2024

NetScaler 控制台的应用分析和管理功能使您能够通过以应用为中心的方法监视应用。这种方法可以帮助您：

- 检查得分并分析应用程序的整体性能
- 检查服务器或客户端是否存在任何问题
- 检测应用程序流量中的异常情况并采取纠正措施

> 注意
>
> 应用程序是指在实例上配置的一个或多个虚拟服务器 (NetScaler)。

您可以监视应用程序的持续时间，例如 1 小时、1 天、1 周和 1 个月。

必备条件

- 确保您已在 NetScaler 控制台中添加了 NetScaler 实例。
- 确保您拥有 NetScaler 实例的有效许可。有关详细信息，请参阅许可。

应用程序概述

应用程序可以是：

- 离散应用
- 自定义应用程序
- 微服务应用程序（k8s_ 离散）

离散应用

在 NetScaler 控制台中发现的所有虚拟服务器都被称为离散应用程序。

自定义应用程序

一个类别下的虚拟服务器称为自定义应用程序。作为管理员，您必须根据类别添加自定义应用程序。然后，您可以通过控制板管理和监视应用程序。您可以轻松监视归类为一个类别的特定应用程序。

例如，您可以为数据中心 1 创建一个类别并添加其 NetScaler 实例。为数据中心 1 定义类别并添加实例后，应用程序控制板将显示一个单独的类别，其中包括与您的数据中心 1 相关的所有应用程序。

需要注意的事项

- 添加到自定义应用程序的离散应用程序将从离散应用程序中删除。
- 所有未添加到任何类别的应用程序都可以作为“其他”。

微服务应用

在 Kubernetes 群集中，NetScaler 为 NetScaler MPX（硬件）、NetScaler VPX（虚拟化）和 NetScaler CPX（容器化）提供 Ingress Controller。有关详细信息，请参阅 NetScaler Ingress Controller。

使用 NetScaler CPX 实例配置的离散应用程序称为微服务应用程序。

Web Insight 控制板

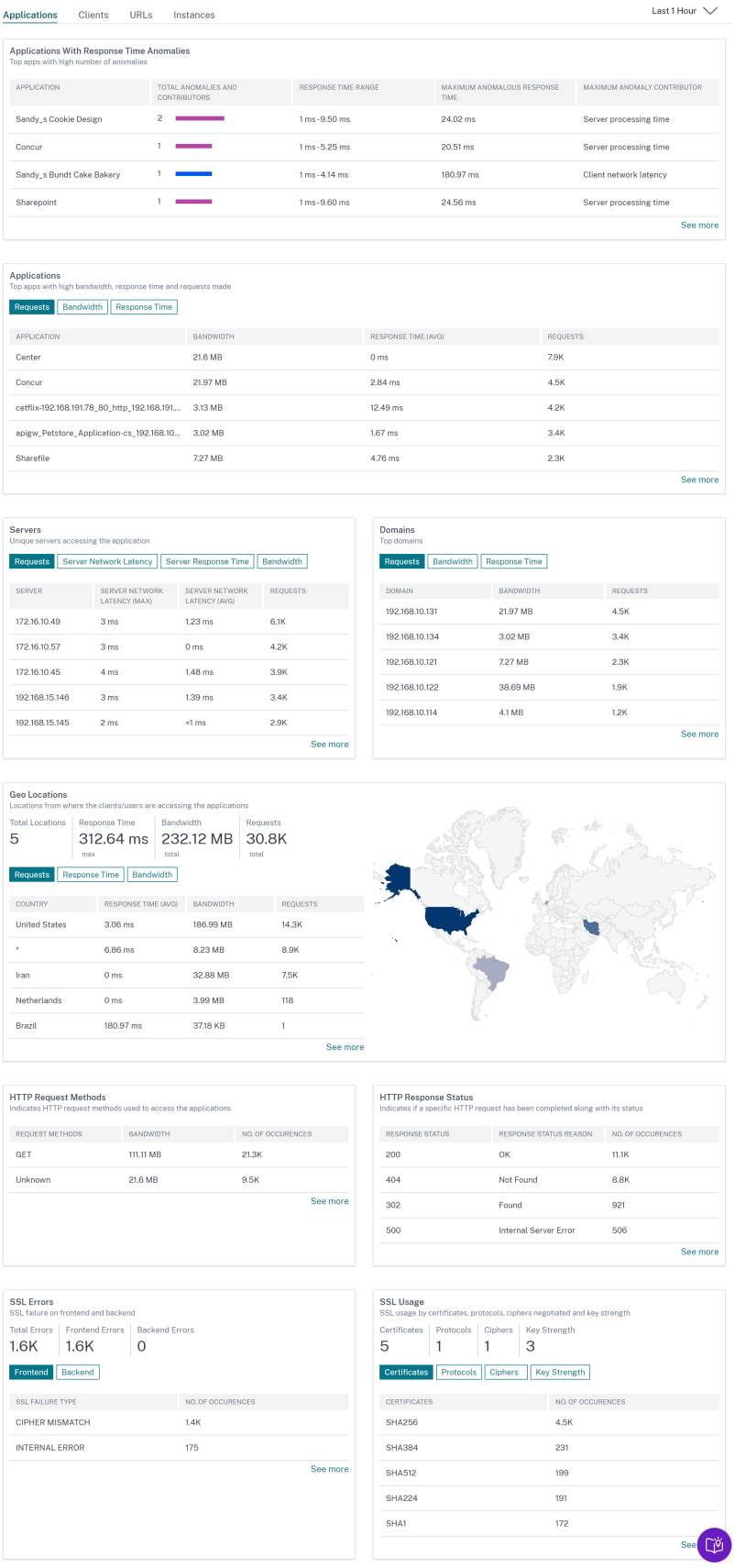
January 29, 2024

改进的 Web Insight 功能得到了增强，并提供了对 Web 应用程序、客户端和 NetScaler 实例的详细指标的可见性。这种改进的 Web Insight 使您能够从性能和使用情况的角度评估和可视化整个应用程序。作为管理员，您可以查看以下内容的 Web Insight：

- 一个应用程序。导航到 应用程序 **>** 控制板，单击应用程序，然后选择 **Web Insight** 选项卡以查看详细指标。有关更多信息，请参阅 应用程序使用情况分析。
- 所有应用程序。导航到 应用程序 **> Web Insight** ，然后单击每个选项卡（应用程序、客户端、实例）以查看以下指标：

应用程序	客户端	URL	实例
具有响应时间异常的应用	客户端	URL	实例指标
应用程序	地理位置		应用程序
服务器	HTTP 请求方法		域
域	HTTP 响应状态		URL
地理位置	URL		HTTP 请求方法
URL	操作系统		HTTP 响应状态
HTTP 请求方法	浏览器		客户端
HTTP 响应状态	SSL 错误		服务器
SSL 错误	SSL 使用情况		操作系统

应用程序	客戶端	URL	实例
SSL 使用情况			浏览器



在每个指标中，您可以查看前 5 个结果。您可以单击进一步向下钻取以分析问题并更快地执行故障排除操作。

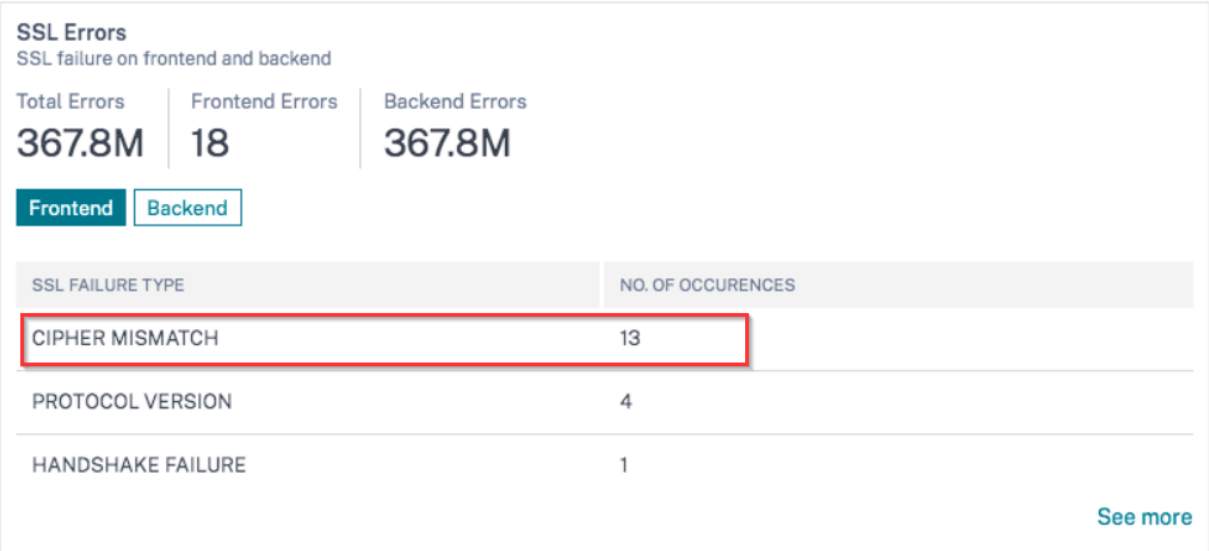
> 注意
>
> - 自 **14.1-1.16** 或更高版本起，当您深入研究某个指标时，时间序列图中的分析视图会显示所选持续时间内的零值（例如，0 毫秒和 0 个请求）。以前，如果在选定的持续时间内没有收到任何流量或交易，则分析视图会跳过这些 nil 值来显示图表。
> - 在某些情况下，NetScaler 可能无法计算某些事务的 RTT 值。对于此类交易，NetScaler 控制台将 RTT 值显示为：
>
> – **NA**—在 NetScaler 实例无法计算 RTT 时显示。
> – **< 1ms**—当 NetScaler 实例以 0 毫秒到 1 毫秒之间的小数计算 RTT 时显示。例如，0.22 毫秒。

查看密码相关问题的详细信息

在 **SSL** 错误下，您可以查看以下 SSL 参数的详细信息：

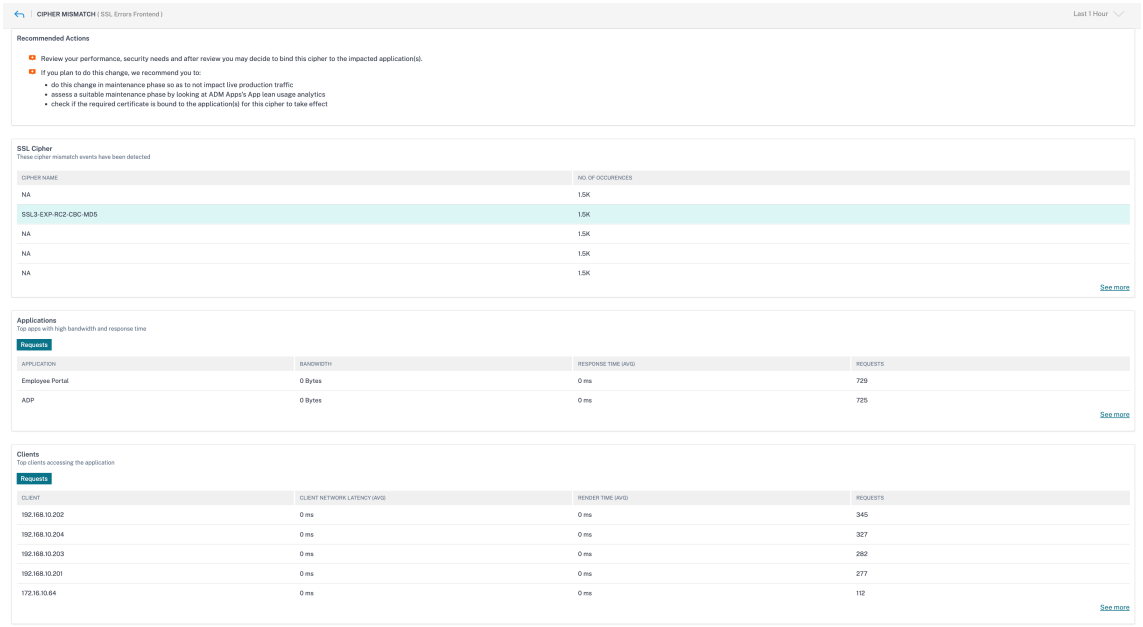
- 密码不匹配
- 不支持的密码

在 **SSL** 错误下，单击 SSL 参数（密码不匹配或不支持的密码）以查看详细信息，例如 SSL 密码名称、推荐操作以及受影响应用程序和客户端的详细信息。

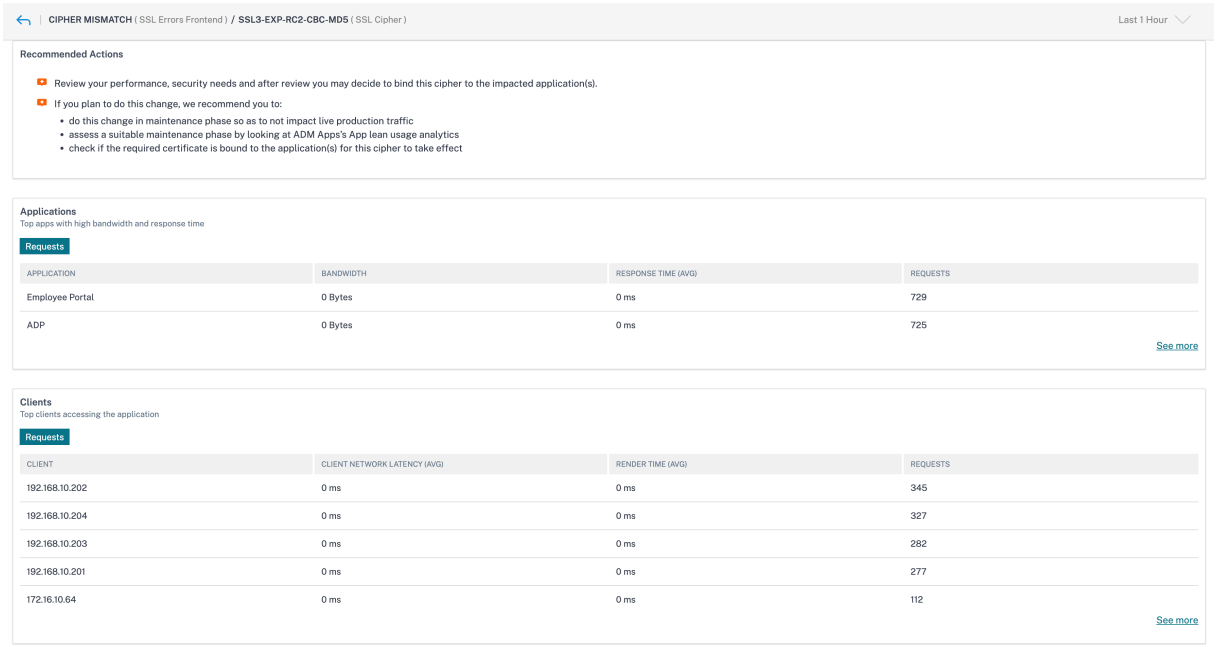


将显示所选 SSL 参数的详细信息页面。您可以：

- 查看“建议的 操作”中提供的建议。
- 在 **SSL** 密码下查看密码名称和出现次数。
- 查看受影响的应用程序和客户端总数。



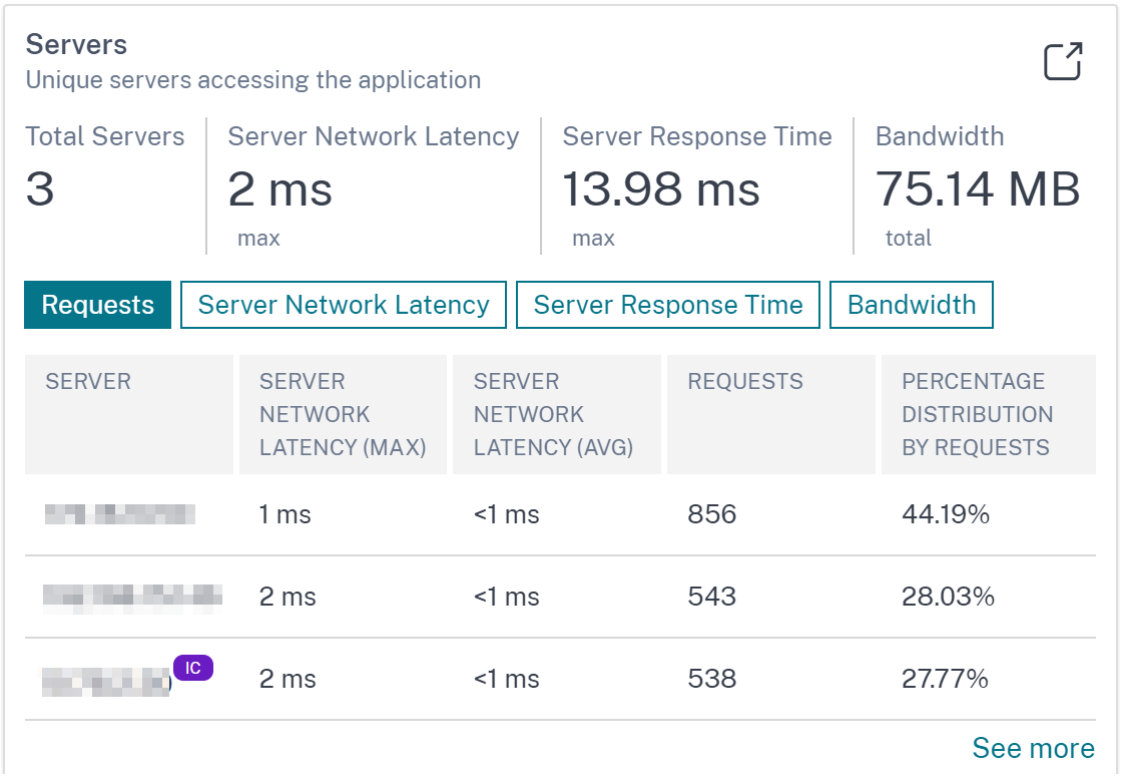
单击 **SSL** 密码名称 可查看受所选 SSL 密码影响的应用程序和客户端。



集成缓存请求

集成缓存在 NetScaler 设备上提供内存存储，无需往返原始服务器即可向用户提供 Web 内容。

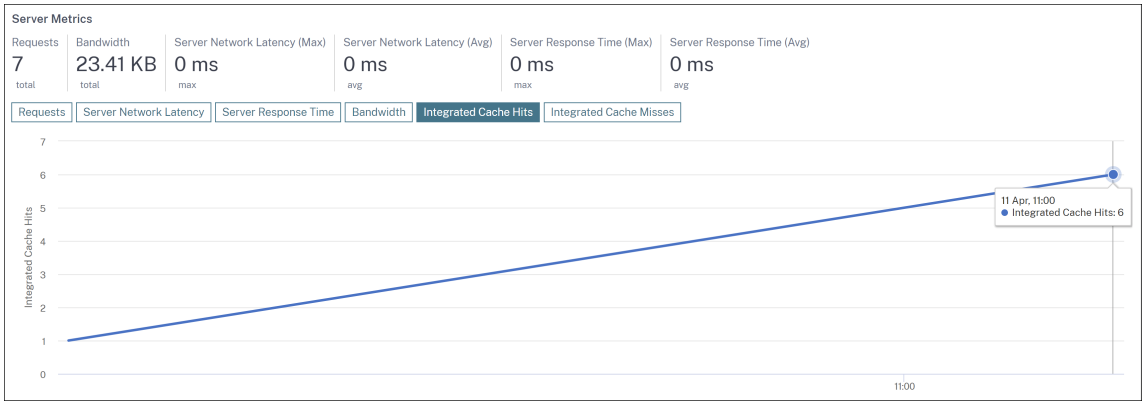
集成缓存请求当前显示在 服务器 下方，NetScaler 虚拟服务器 IP 地址旁边有一个 IC 通知。使用源服务器 IP 地址，所有其他请求都可见。



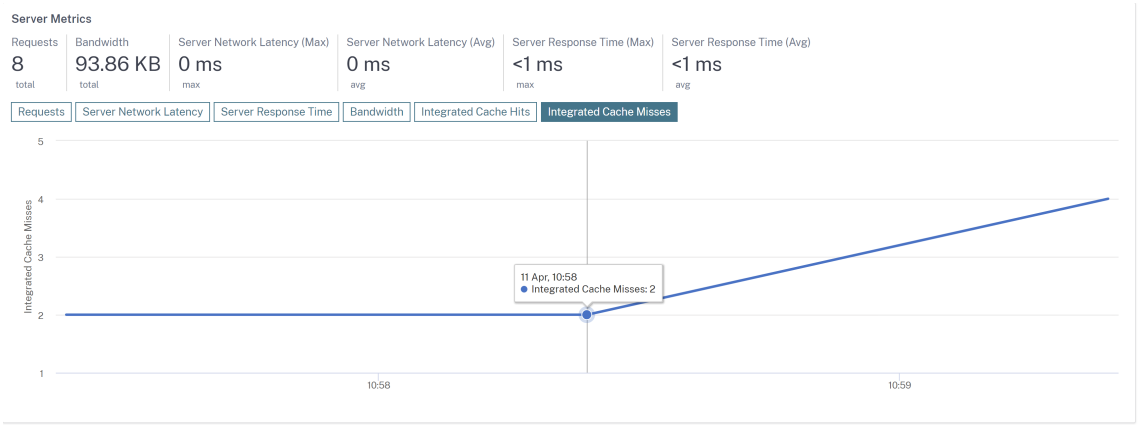
当您深入查看服务器以查看更多详细信息时，服务器指标会显示集成的缓存命中率和未命中率选项卡。

以下对象中的图表视图：

- 在集成缓存命中率选项卡中，您可以查看 NetScaler 设备从缓存中提供的响应总数。



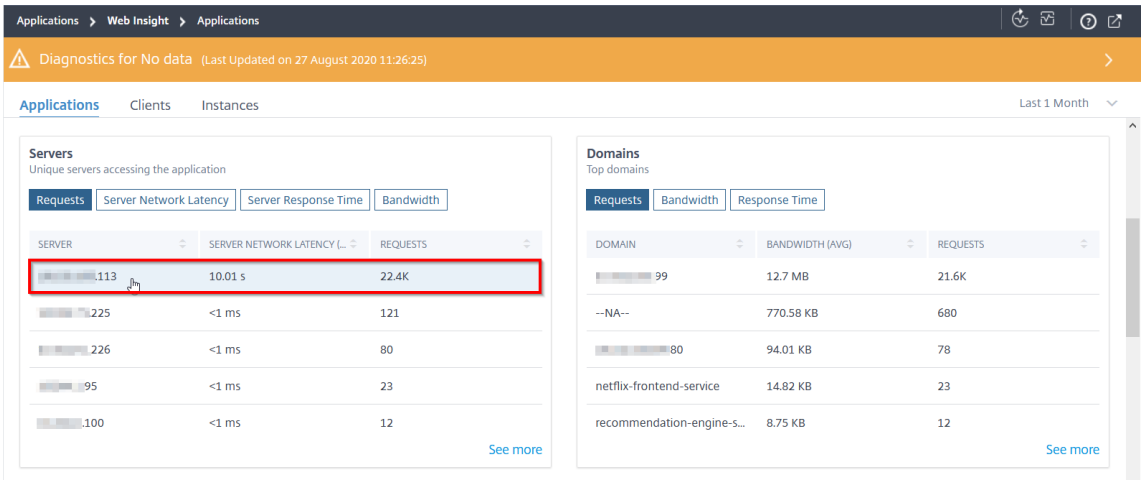
- 在集成缓存未命中选项卡中，您可以查看 NetScaler 设备从源服务器提供的响应总数。



其他用例

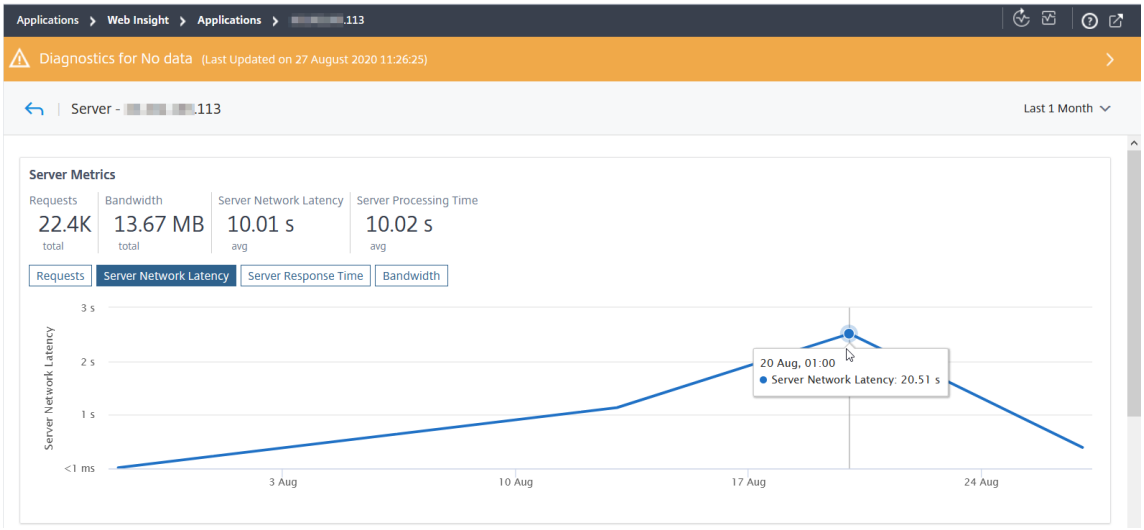
假设您要分析 1 个月的服务器网络延迟，然后决定是扩大还是缩小生产环境。要分析这个：

1. 从列表中选择过去 1 个月，然后从 应用程序 选项卡中选择，向下滚动到服务 器，然后单击服务器。



将显示所选服务器的度量详细信息。

2. 选择“服务器网络延迟”选项卡以分析延迟。



平均延迟表示 10.01 秒，从图表中，您可以分析过去 1 个月的服务器网络延迟似乎很高。作为管理员，您可以决定扩大生产环境。

分析应用程序缓慢的根本原因

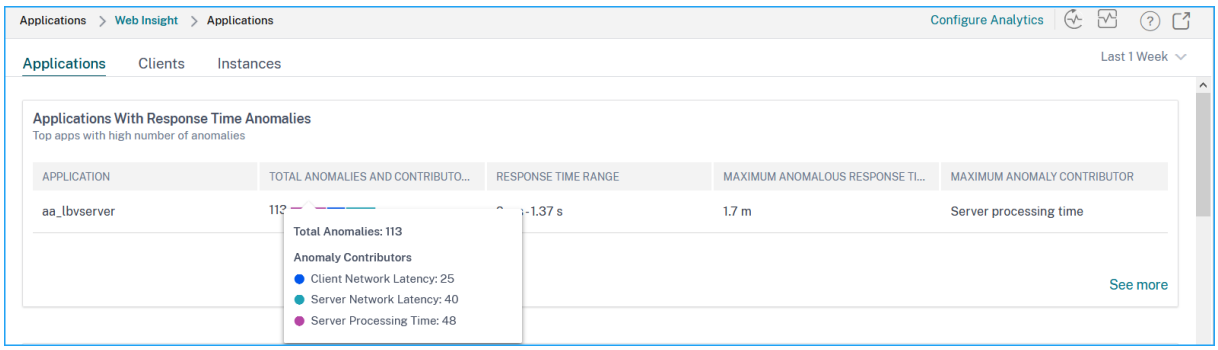
January 29, 2024

应用程序缓慢是任何组织的一个主要问题，因为它会导致业务影响或生产效率。作为管理员，您必须确保所有应用程序都能以最佳方式运行，以避免任何业务影响。当您的用户在访问应用程序时遇到速度缓慢时，必须确保问题是否存在于：

- 客户端网络延迟
- 服务器网络延迟
- 服务器处理时间

NetScaler 控制台每小时执行一次异常检查，并根据某些前提条件报告过去 1 小时流量的异常情况。例如，为了避免误报结果，如果响应时间小于 1 毫秒，则会跳过这些结果的异常检查。

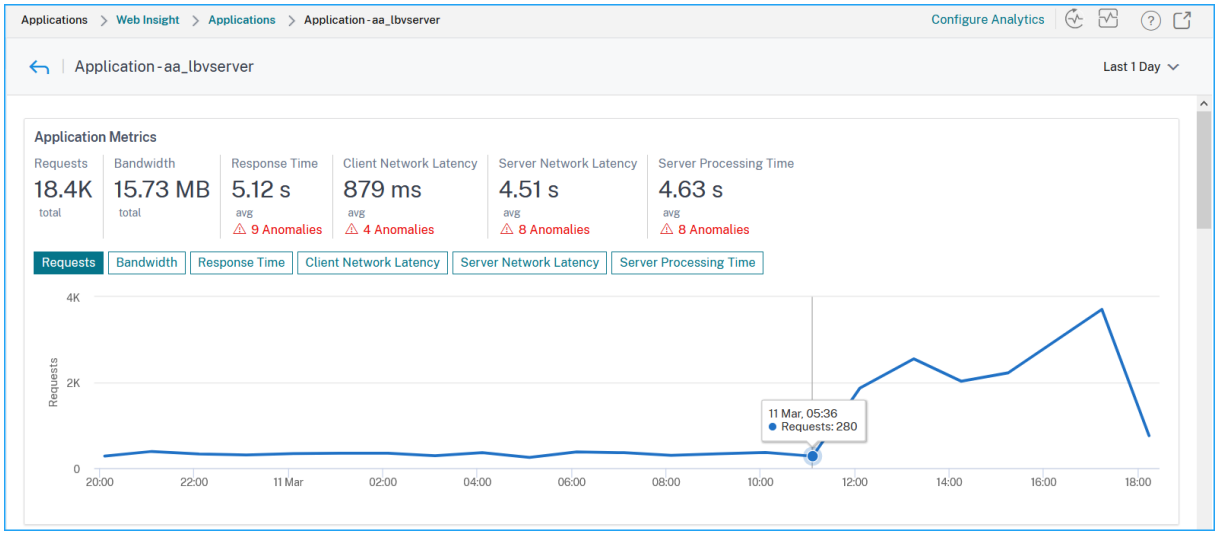
使 用“应用程序”**>** “**Web Insight**”页面，您可以查看在选定持续时间内具有响应时间异常的应用程序。“具有响应时间异常的应用 程序”度量根据总异常情况显示前五个应用程序。单击查 看更多 以查看所有应用程序。



- 应用程序—表示应用程序名称。
- 总异常和贡献者—表示应用程序中的总异常情况。当鼠标指针悬停时，您可以分别查看来自客户端网络延迟、服务器网络延迟和服务器处理时间的总异常情况。
- 响应时间范围—表示应用程序的预期响应时间范围。
- 最大异常响应时间—表示应用程序的最长响应时间。
- 最大异常参与者—表示应用程序的最大异常数是来自客户端网络延迟、服务器网络延迟还是服务器处理时间。

应用程序向下钻取

单击应用程序以查看所选持续时间的 应用程序指标 详细信息。



应用程序指标 使您能够查看：

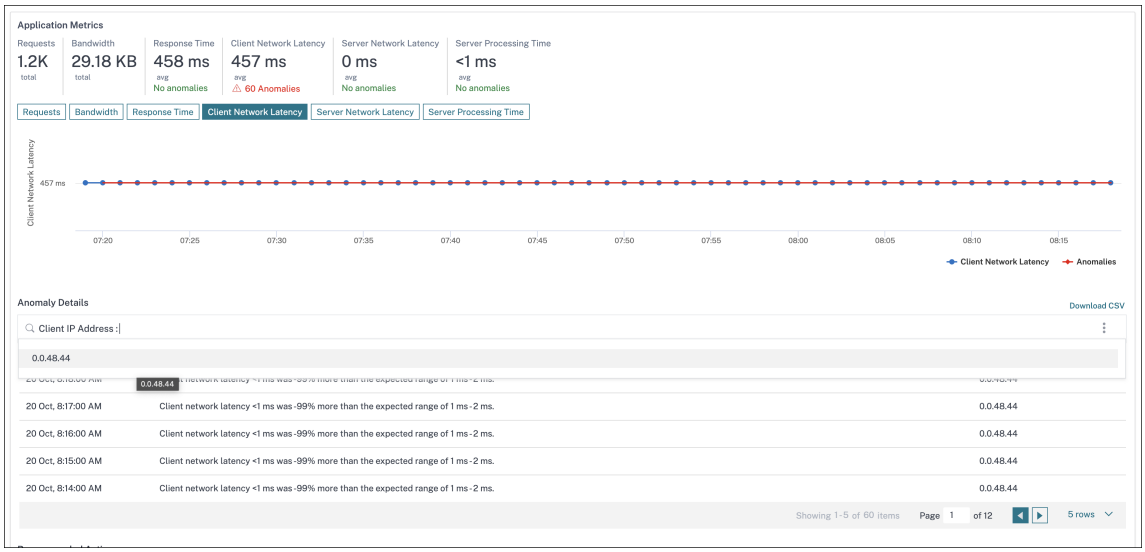
- 摘要—可视化应用程序性能的概述，例如响应时间、请求和带宽
- 请求 - 应用程序收到的请求总数。还可以根据请求总数查看来自前 5 个客户端的请求
- 带宽 - 应用程序处理的总带宽。还可以根据总带宽消耗量查看前 5 台服务器的带宽消耗
- 响应时间—在同一张图上可视化客户端网络延迟、服务器网络延迟和服务器处理时间的概述

- 客户端网络延迟—平均客户端网络延迟（从客户端到 NetScaler）
- 服务器网络延迟—服务器网络的平均延迟（从 NetScaler 到服务器）
- 服务器处理时间—平均服务器处理时间（从服务器到 NetScaler）

如果应用程序存在异常，则可以查看异常是来自客户端网络延迟、服务器网络延迟还是服务器处理时间。单击每个选项卡查看详细信息。

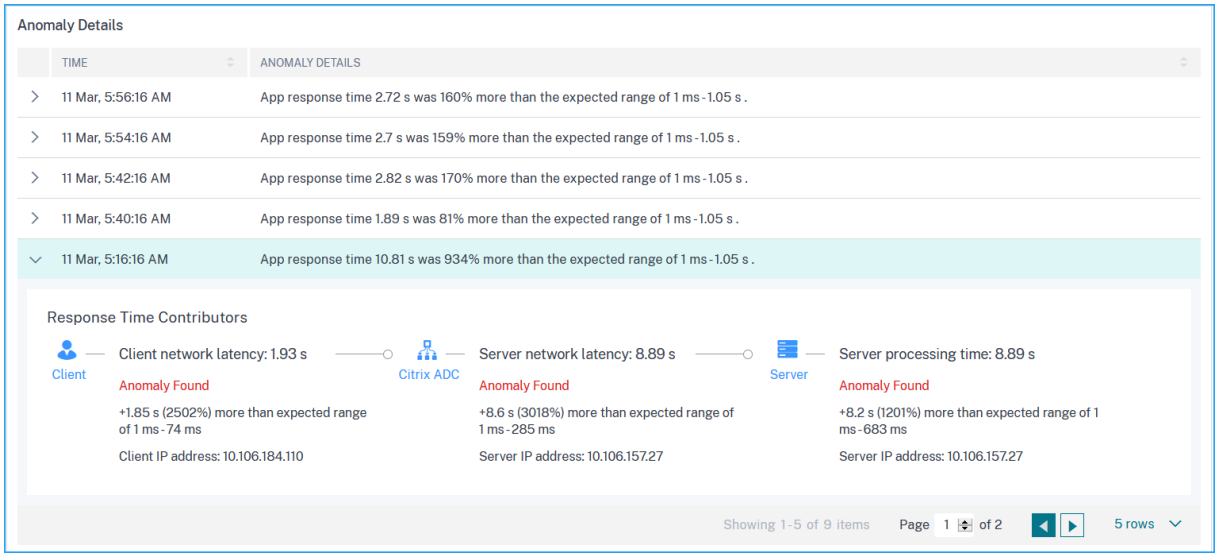
在“客户端网络延迟”和“服务器网络延迟”选项卡中，您可以查看：

- 搜索栏 - 单击搜索栏可查看所有客户端（在“客户端网络延迟”中）和服务器（在“服务器网络延迟”中）的 IP 地址。您可以选择 IP 地址来筛选结果。
- 导出选项 -单击“下载 **CSV**”以 CSV 格式导出详细信息。

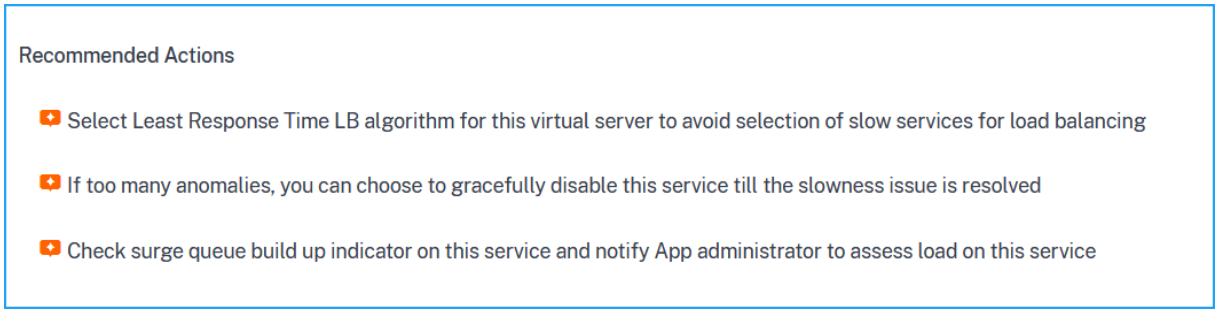


响应时间

在“异常详细信息”下，单击以查看响应时间贡献者的详细信息（从客户端到服务器）。以下示例存在客户端网络延迟、服务器网络延迟和服务器处理时间的异常情况。您还可以查看预期范围以及超出预期范围的违规行为。



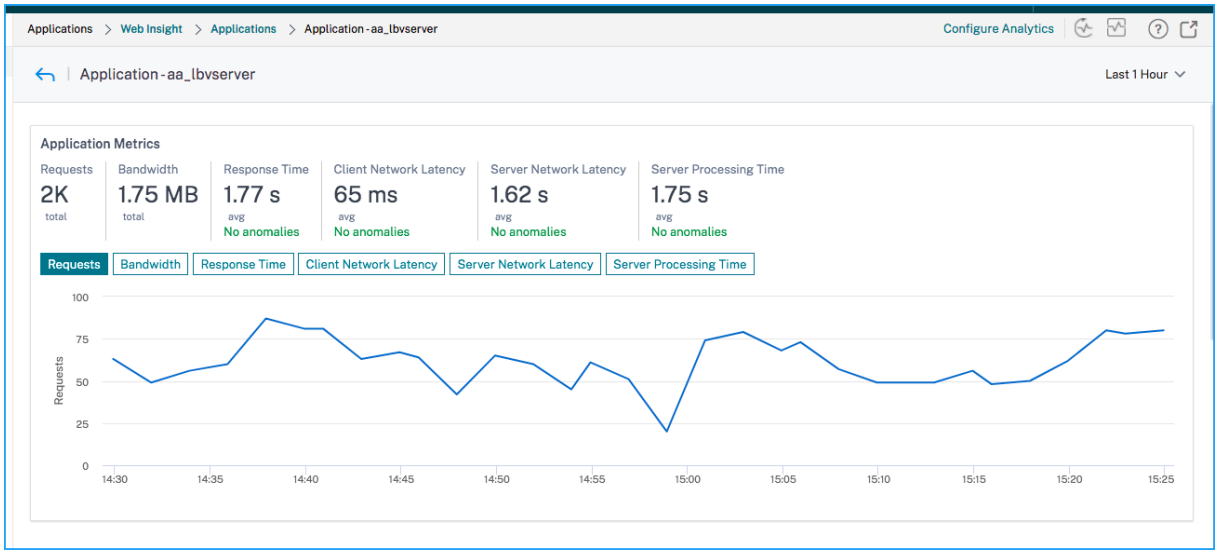
建议的操作 建议您解决异常情况的可能解决方案。



同样，您可以单击 客户端网络延迟、服务器网络延迟和 服务器处理时间 选项卡以查看：

- 已经超过预期范围的异常情况。
- 建议您采取可能的解决方案的操作。

如果应用程序性能良好，则可以将应用程序指标视为没有异常。



服务图表

March 10, 2024

NetScaler 控制台中的服务图功能使您能够以图形表示方式监视所有 Kubernetes 服务。此功能还允许您查看服务的详细分析和可操作指标。导航到应用程序 **>** 服务图表以查看以下内容的服务图表：

- 跨所有 NetScaler 实例配置的应用程序
- Kubernetes 应用程序
- 3 层 Web 应用程序

跨所有 **NetScaler** 实例的应用程序的服务图表

通过全球服务图表功能，您可以获得 `clients to infrastructure to application` 视图的整体可视化。在此单窗格服务图表视图中，作为管理员，您可以：

- 了解用户从哪个区域访问特定应用程序（3 层 Web 应用程序和微服务应用程序）
- 可视化处理客户端请求的基础结构（NetScaler 实例）视图
- 了解问题是来自客户端、基础结构还是应用程序
- 进一步深入解决问题

导航到应用程序 **>** 服务图表，然后单击全局选项卡以查看：

- 从客户端到后端服务器连接的所有应用程序的端到端
- 连接到各自数据中心的所有 NetScaler 实例

> 注意
>
> 只有在拥有 GSLB 应用程序时，才能查看数据中心。

- 客户端指标信息
- NetScaler 指标信息
- 所有具有离散应用程序、定制应用程序和离散微服务应用程序的 NetScaler 实例
- 属于自定义应用程序、离散应用程序和微服务应用的前 4 个低分应用
- 排名前 4 位低分虚拟服务器的指标信息
- 应用程序（离散应用程序、自定义应用程序和微服务应用程序）状态如“严重”、“评论”、“良好”和“不适用”

有关详细信息，请参阅服务图表中的应用程序的整体视图。

Kubernetes 应用程序的服务图表

导航到应用程序 **>** 服务图表，然后单击微服务选项卡以：

- 确保端到端应用程序的整体性能
- 识别因应用程序不同组件之间的相互依赖性而造成的瓶颈
- 收集对应用程序不同组件依赖关系的见解
- 监视 Kubernetes 群集中的服务
- 监视哪个服务有问题
- 检查导致性能问题的因素
- 查看服务 HTTP 事务的详细可见性
- 分析 HTTP、TCP 和 SSL 指标
- 查看客户指标和客户交易摘要详情

通过在 NetScaler 控制台中可视化这些指标，您可以分析问题的根本原因并更快地采取必要的故障排除措施。服务图表将应用程序显示到各种组件服务中。在 Kubernetes 群集内运行的这些服务可以与应用程序内外的各种组件进行通信。要开始使用，请参阅设置服务图表。

3 层 **Web** 应用程序的服务图表

导航到应用程序 **>** 服务图表，然后单击 **Web** 应用程序 选项卡以查看：

- 有关如何配置应用程序的详细信息（使用内容交换虚拟服务器和负载平衡虚拟服务器）

  对于 GSLB 应用程序，您可以查看数据中心、NetScaler 实例、CS 和 LB 虚拟服务器。

- 从客户端到服务的端到端事务
- 客户端访问应用程序的位置
- 处理客户端请求的数据中心名称和关联的数据中心 NetScaler 指标（仅适用于 GSLB 应用程序）
- 客户端、服务和虚拟服务器的度量详细信息
- 如果错误来自客户端或服务
- 服务状态，例如“严重”、“审核”和“良好”。NetScaler 控制台根据服务响应时间和错误数量显示服务状态。
  - 严重（红色） -表示平均服务响应时间大于 200 毫秒且错误计数 > 0
  - 查看（橙色） -表示平均服务响应时间大于 200 毫秒或错误计数 > 0
  - 良好（绿色） -表示没有错误，平均服务响应时间小于 200 毫秒
- 客户端状态，例如“严重”、“审阅”和“良好”。NetScaler 控制台根据客户端网络延迟和错误数量显示客户端状态。
  - 严重（红色）-指示客户端网络平均延迟大于 200 毫秒且错误计数 > 0
  - 查看（橙色） -指示客户端网络平均延迟 > 200 毫秒或错误计数 > 0
  - 良好（绿色） -表示无错误且客户端网络平均延迟小于 200 毫秒
- 虚拟服务器的状态，例如“严重”、“审核”和“良好”。NetScaler 控制台根据应用程序评分显示虚拟服务器状态。
  - 严重（红色） -表示应用得分小于 40 时
  - 评价（橙色） -表示应用得分介于 40 和 75 之间的情况
  - 良好（绿色） -指示应用程序得分大于 75

注意事项：

- 服务图中仅显示负载平衡、内容切换和 GSLB 虚拟服务器。
- 如果没有将虚拟服务器绑定到自定义应用程序，则详细信息在应用程序的服务图中不可见。
- 只有在虚拟服务器和 Web 应用程序之间发生活动事务时，才能在服务图中查看客户端和服务的度量。
- 如果虚拟服务器和 Web 应用程序之间没有活动事务处理，则只能根据配置数据（如负载平衡、内容切换、GSLB 虚拟服务器和服务）在服务图中查看详细信息。
- 如果对应用程序配置进行了任何更改，则可能需要 10 分钟才能反映在服务图中。

有关详细信息，请参阅 应用程序的服务图。

样书

January 29, 2024

样书简化了为应用程序管理复杂的 NetScaler 配置的任务。样书是可以用来创建和管理 NetScaler 配置的模板。

使用样书，您可以：

- 配置 NetScaler 的特定功能。
- 为 Microsoft Exchange 或 Lync 等企业应用程序部署创建配置。

样书非常符合 DevOps 团队实践的基础结构即代码原则，其中，配置是声明性且版本受控的。配置还是重复使用的，并作为整体部署。样书具有以下优势：

- 声明式：样书是用声明式语法而不是命令式语法编写的。样书允许您专注于描述配置的结果或“所需状态”，而不必详细说明如何在特定 NetScaler 实例上实现配置的分步说明。NetScaler 控制台计算 NetScaler 上的现有状态与您指定的所需状态之间的差异，并对基础架构进行必要的编辑。由于样书使用以 YAML 编写的声明性语法，因此样书的组件可以按任意顺序指定，NetScaler 控制台根据其计算的依赖关系来确定正确的顺序。
- 原子：使用样书部署配置时，将部署完整配置或不部署任何配置，这可确保基础结构始终处于一致状态。
- 版本化：样书具有将其与系统中的任何其他样书唯一区分开的名称、命名空间和版本号。对样书进行任何修改均需要更新其版本号（或者其名称或命名空间）以维护此唯一特征。此外，通过版本更新可以维护同一样书的多个版本。
- 可组合：定义了样书后，可以将该样书用作构建其他样书的单元。您可以避免重复使用配置的公用模式。此外，通过它您还可以在您的组织中建立标准构建块。由于样书是版本化的，因此，对现有样书进行更改会产生新的样书，从而确保绝不会意外破坏依赖样书。
- 以应用程序为中心：样书可用于定义完整应用程序的 NetScaler 配置。可以使用参数提取应用程序的配置。因此，基于样书创建配置的用户可以与一个简单界面交互，包括填写一些参数来创建复杂的 NetScaler 配置。基于样书创建的配置不绑定到基础结构。因此，单个配置可以部署在一个或多个 NetScaler 实例上，也可以在实例之间移动。
- 自动生成的用户界面：当使用 NetScaler 控制台 GUI 完成配置时，NetScaler 控制台会自动生成用户界面表单，用于填写样书的参数。样书作者无需了解新的 GUI 语言或单独创建 UI 页面和表单。
- **API** 驱动：使用 NetScaler 控制台 GUI 或 REST API 支持所有配置操作。可以在同步模式或异步模式下使用 API。除了配置任务外，通过样书 API 还可以在运行时发现任何样书的架构（参数说明）。

可以使用一个样书创建多个配置。每个配置都保存为一个配置包。例如，假设有一个定义典型 HTTP 负载平衡应用程序配置的样书。您可以使用负载平衡实体的值创建配置，然后在 NetScaler 实例上运行。此配置保存为一个配置包。您可以使用同一样的样书来创建具有不同值的另一个配置，然后在相同或不同的实例上运行它。即为此配置创建一个新配置包。配置包既保存在 NetScaler 控制台上，也保存在运行配置的 NetScaler 实例上。

您可以使用 NetScaler 控制台附带的默认样书为部署创建配置，也可以设计自己的样书并将其导入到 NetScaler 控制台。您可以使用 NetScaler 控制台 GUI 或使用 API 使用样书来创建配置。

本文档包括以下几个部分：

- 如何查看样书
- 默认样书
- 为业务应用程序开发的样书
- 自定义样书
- 样书中的 API
- 样书语法

“应用程序安全性”控制板

March 10, 2024

应用程序安全性控制面板为您提供了已发现应用程序的安全指标概览。此控制板显示已发现应用程序的安全攻击信息，例如同步攻击、小窗口攻击、DNS 洪水攻击。

要查看应用程序安全控制板上的安全指标，请执行以下操作：

1. 导航到“安全”**>**“安全控制面板”。
2. 从实例列表中选择实例 IP 地址。

   报告包含每个应用程序的以下信息：

   - 威胁指数。一个单位数评级系统，用于指示应用程序攻击的严重程度。应用程序上的攻击越严重，该应用程序的威胁指数越高。值范围介于 1 到 7 之间。

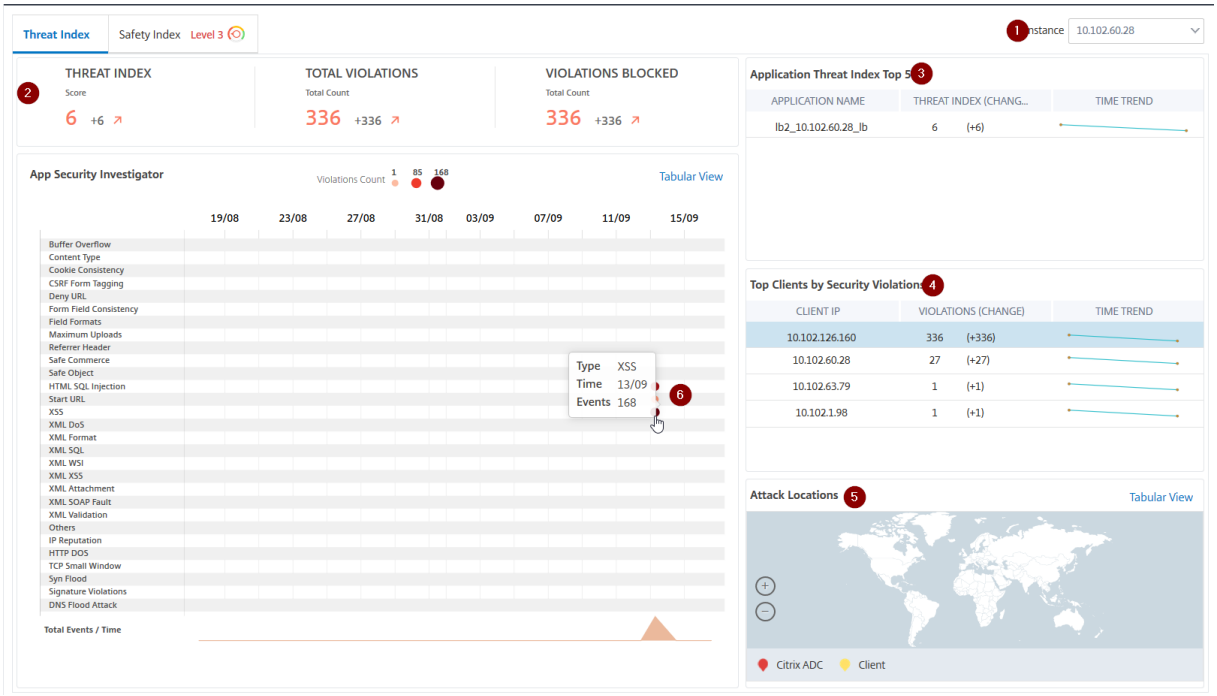
     威胁指数基于攻击信息。与攻击相关的信息，例如违规类型、攻击类别、位置和客户端详细信息，可以深入了解对应用程序的攻击。只有在违规或攻击发生时，违规信息才会发送到 NetScaler 控制台。许多漏洞和漏洞导致了高威胁指数值。

   - 安全指数。一个单位数评级系统，用于指示您配置 NetScaler 实例以保护应用程序免受外部威胁和漏洞的安全性。应用程序的安全风险越低，安全指数越高。值范围介于 1 到 7 之间。

     安全指标同时考虑应用程序防火墙配置和 NetScaler 系统安全配置。为了获得较高的安全指数值，两个配置都必须强健。例如，如果实施了严格的应用程序防火墙检查，但是 NetScaler 系统安全措施（例如未为 nsroot 用户提供强密码），则会为应用程序分配一个较低的安全指数值。

您可以查看 应用程序安全调查器上报告的差异。

威胁索引详细信息



1 -显示您可以查看其详细信息的 NetScaler 实例 IP 地址。

2 -显示威胁指数得分、发生的违规总数和阻止的违规总数等详细信息。

3 -显示所选实例的虚拟服务器。

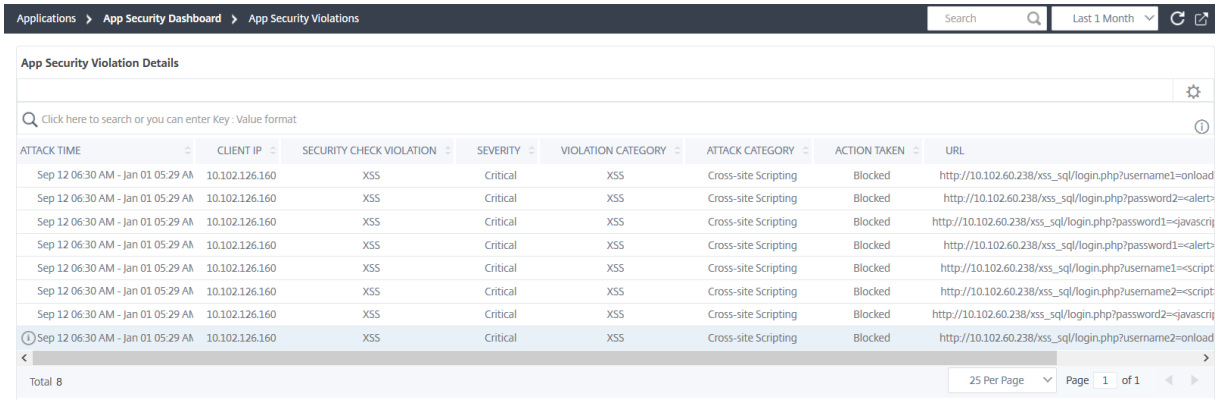
4 -显示基于客户端的安全违例。将显示每个客户端的“应用安全调查器”图形。您可以单击每个客户端 IP 以查看结果。

5 -在地图视图和表格视图中显示违规。

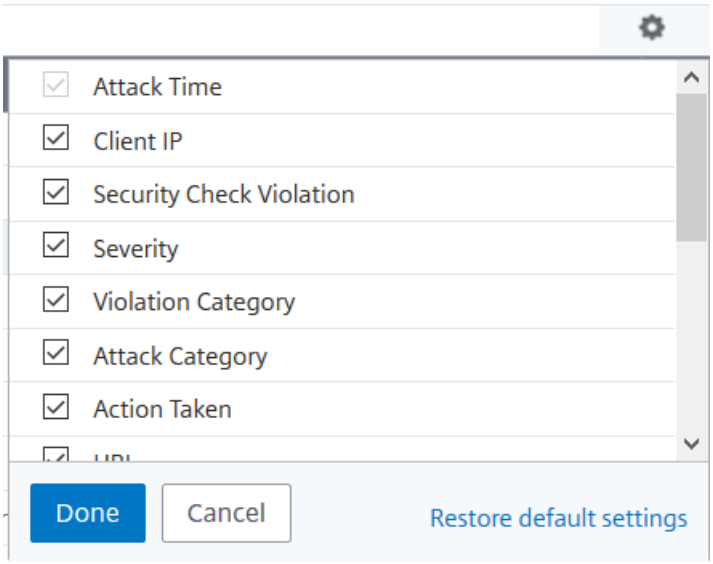
6 -显示违规详情。将鼠标指针悬停在图形上时，将显示违规类型、攻击时间和总事件等详细信息。

单击气泡图时，详细信息将显示在 应用程序安全违规详细信息 页面中。例如，如果要进一步查看跨站点脚本违规的详细信息，请在 应用程序安全调查器 中单击为 **XSS** 填充的图表。

显示应用程序安全违例详细信息，包括攻击时间、攻击类别、严重程度、URL 等违例详细信息。



您还可以单击设置选项以选择要显示的选项。



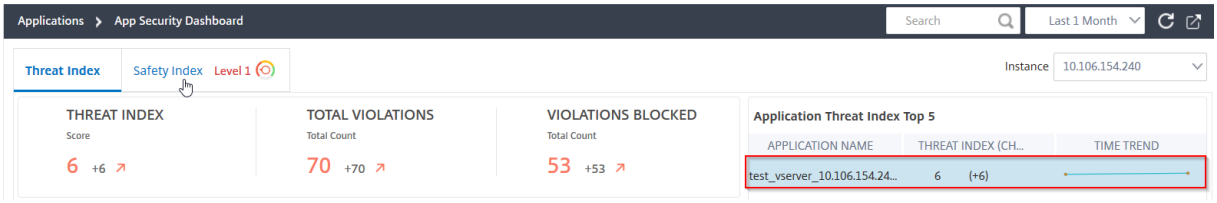
安全指数详细信息

查看了应用程序面临的威胁后，您希望确定哪些应用程序安全配置正在实施，以及该应用程序缺少哪些配置。您可以通过深入查看应用程序安全指数摘要来获取此信息。

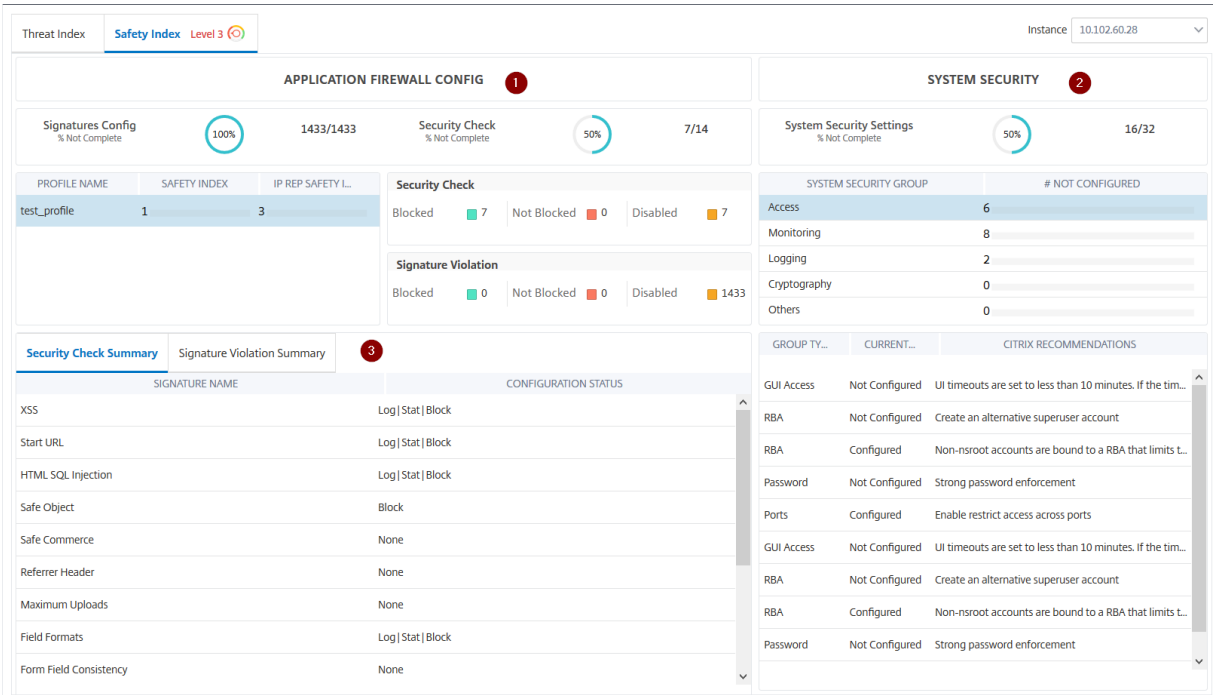
安全指数摘要为您提供有关以下安全配置的有效性：

- 应用程序防火墙配置。显示多少签名和安全实体未配置。
- **NetScaler** 控制台系统安全。显示多少系统安全设置未配置。

要查看安全指数详细信息，请选择虚拟服务器/应用程序，然后单击安全指数选项卡。



将显示详细信息。



1 -显示应用程序防火墙配置的详细信息。

2 -显示系统安全性的详细信息。单击每个安全组以获取有关状态和 Citrix 建议的详细信息。

3 -显示安全检查和签名违规的摘要。

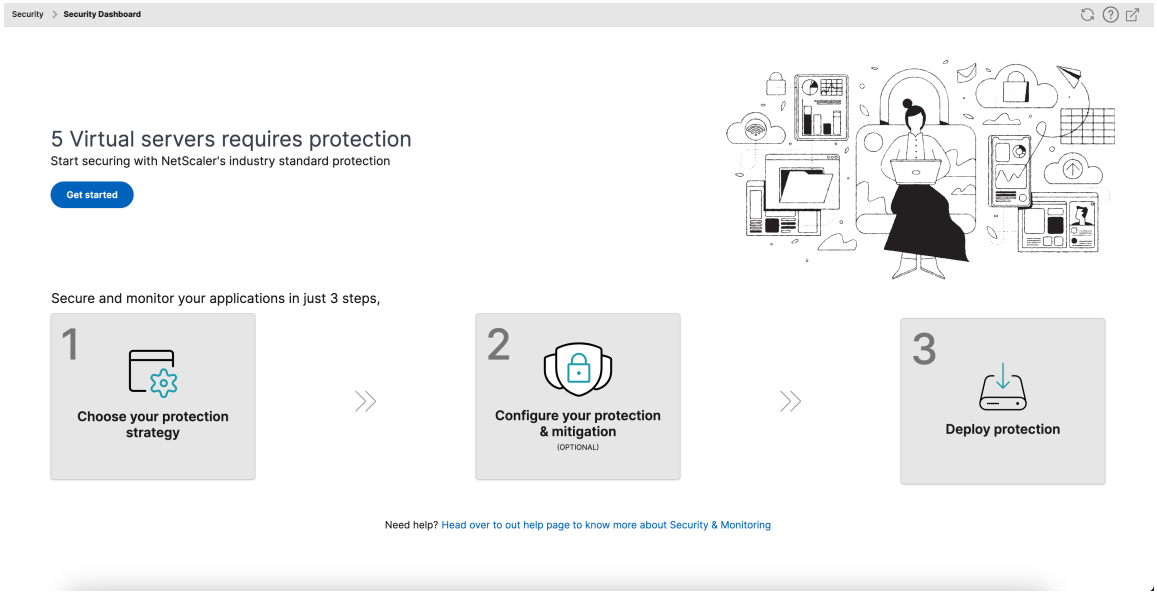
您还可以通过启用虚拟服务器 的安全洞察然后导航到“安全”**>**“安全违规”来查看威胁环境的摘要。有关安全指数用例的更多信息，请参阅安全洞察。

“统一安全”控制面板

March 10, 2024

统一安全控制面板是一个单窗格控制板，您可以在其中配置保护、启用分析并在应用程序上部署保护。在此控制板中，您可以从各种模板选项中进行选择，并在单个工作流程中完成整个配置过程。要开始使用，请导航到“安全”**>**“安全控制面板”，然后单击“管理应用程序”。在 管理应用程序 页面中，您可以查看安全和不安全应用程序的详细信息。

> 注意：
>
> - 如果您是新用户，或者您没有通过样书或直接在 NetScaler 实例上配置任何保护，则在单击“安全”**>**“安全控制面板”后会显示以下页面。

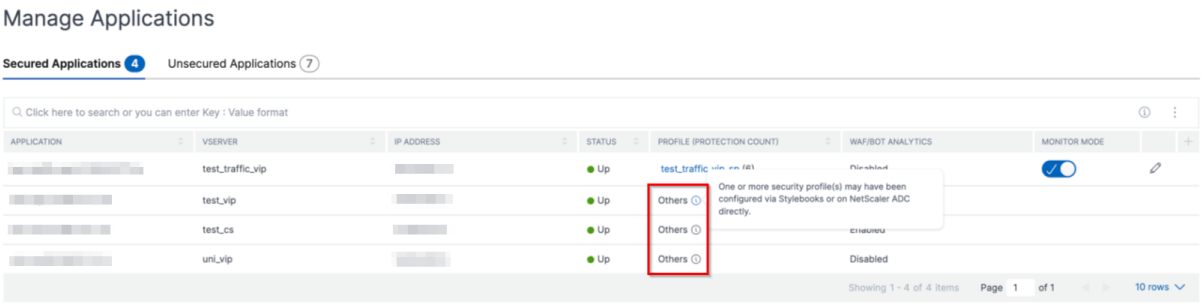


- 您可以查看需要保护的虚拟服务器的总数。单击“开始”可在“不安全的应用程序”中查看详细信息。
- 符合配置保护条件的虚拟服务器类型是负载平衡和内容切换。

安全的应用程序

在使用统一安全控制面板配置保护后，您可以查看详细信息。有关更多信息，请参阅 为不安全的应用程序配置保护。

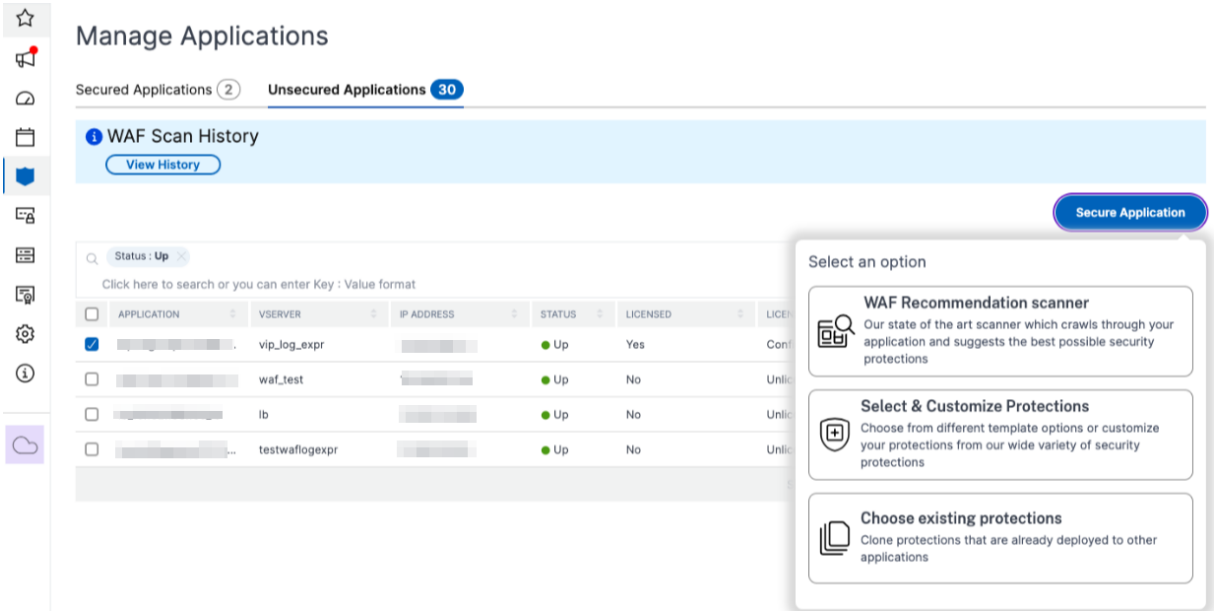
如果您已经直接在 NetScaler 实例上或通过样书配置了保护，则可以在“配置文件”下标记为“其他”的“安全应用程序”选项卡中查看这些应用程序。



为不安全的应用程序配置保护

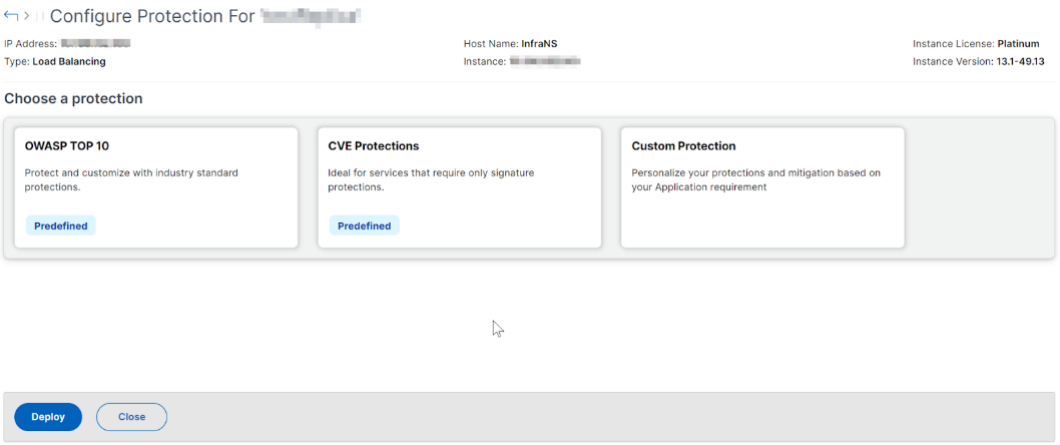
> 注意：
>
> 阻止列表中支持的最大配置实体（规则）为 32。

在“不安全的应用程序”选项卡中，选择一个应用程序，然后单击“安全应用程序”。



您可以选择以下任一选项来保护您的应用程序：

- WAF 推荐扫描器 -此选项使您能够对应用程序运行扫描。根据扫描的某些参数，结果会提示您对应用程序的保护。您可以考虑应用这些建议。
- 选择和自定义保护 -此选项使您可以从不同的模板选项中进行选择或自定义保护和部署。



  - **OWASP** 前 **10** 名 -一种预定义的模板，具有行业标准保护，可防御 OWASP 十大安全风险。有关详细信息，请参阅 https://owasp.org/www-project-top-ten/。
  - **CVE** 保护 -您可以从按已知漏洞类别分类的预配置签名规则列表中创建签名集。当签名模式与传入流量匹配时，您可以选择签名来配置日志或屏蔽操作。日志消息包含漏洞的详细信息。
  - 自定义保护 -选择保护并根据您的要求进行部署。
- 选择现有保护 -此选项克隆部署在现有应用程序中的保护。如果要将相同的保护部署到其他应用程序，则可以选择此选项并将其按原样部署到另一个应用程序。您也可以选择此选项作为模板，修改保护，然后部署。

WAF 推荐扫描器

> 注意：
>
> - 一次只能对一个应用程序运行一次扫描。要开始对同一应用程序或其他应用程序进行新的扫描，必须等到先前的扫描完成。
> - 您可以单击“查看历史记录”来查看过去扫描的历史记录和状态。您也可以单击“查看报告”，然后稍后应用建议。

必备条件：

- NetScaler 实例 必须是 13.0 41.28 或更高版本（用于安全检查）和 13.0 或 更高版本（用于签名）。
- 必须拥有高级许可证。
- 必须是负载平衡虚拟服务器。

要开始使用 WAF 推荐扫描，您必须提供以下信息：

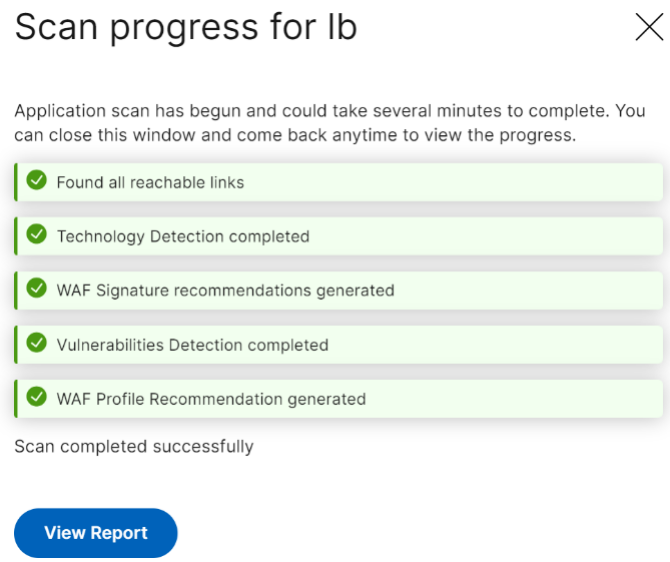
1. 在“扫描参数”下：
   - 域名 -指定有效的可访问 IP 地址或与应用程序关联的可公开访问的域名。例如：`www.example.com`。
   - **HTTP/HTTPS** 协议 -选择应用程序的协议。
   - 流量超时 -扫描期间单个请求的等待时间（以秒为单位）。该值必须大于 0。
   - 开始扫描的 **URL** -启动扫描的应用程序的主页。例如，`https://www.example.com/home`。URL 必须是有效的 IPv4 地址。如果 IP 地址是私有的，则必须确保可以从 NetScaler 控制台管理 IP 访问私有 IP 地址。
   - 登录 **UR** L —用于身份验证的登录数据发送到的 URL。在 HTML 中，此 URL 通常被称为操作 URL。
   - 身份验证方法 -为您的应用程序选择支持的身份验证方法（基于表单或基于标题）。
     - 基于表单的身份验证需要使用登录凭据向登录 URL 提交表单。这些凭据必须采用表单字段及其值的形式。然后，应用程序共享用于在扫描期间维护会话的会话 cookie。
     - 基于标头的身份验证需要标头部分中的身份验证标头及其值。身份验证标头必须具有有效值，用于在扫描期间维护会话。表单字段应留空以用于基于标题。
   - 请求方法 -选择向登录 URL 提交表单数据时使用的 HTTP 方法。允许的请求方法是 **POST**、**GET** 和 P **UT**。
   - 表单字段—指定要提交到登录 URL 的表单数据。只有选择基于表单的身份验证时，表单字段才是必填字段。您必须在键值对中指定，其中字段名是“键”，字段值是“值”。确保正确添加登录所需的所有表单字段，包括密码。这些值在存储到数据库之前经过加密。您可以单击“添加”来添加多个表单域。例如，字段名称 -用户名和 字段值 -管理员。

- 注销 **URL** -指定访问后终止会话的 URL。例如：`https://www.example.com/customer/logout`。

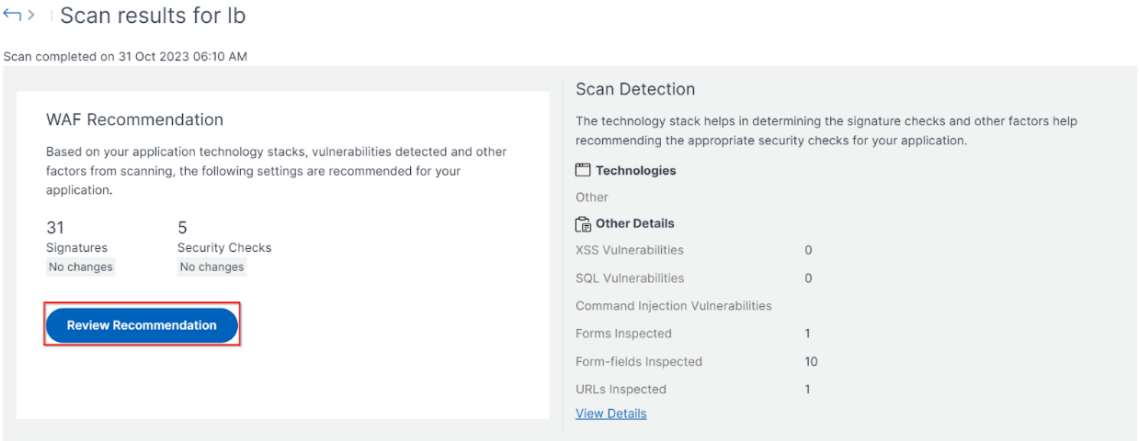
2. 在“扫描配置”下：

   - 要检查的漏 洞-选择漏洞，让扫描程序进行检测。目前，这是针对 SQL 注入和跨站点脚本冲突执行的。默认情况下，所有违规行为均处于选中状态。选择漏洞后，它会模拟对应用程序的这些攻击，以报告潜在的漏洞。建议启用不在生产环境中的这种检测。还报告了所有其他漏洞，但没有模拟对应用程序的这些攻击。
   - 响应大小限制 -响应大小的最大限制。不扫描超过上述值的任何响应。建议的限制为 10 MB（1000000 字节）。
   - 请求并发 -并行发送到 Web 应用程序的请求总数。

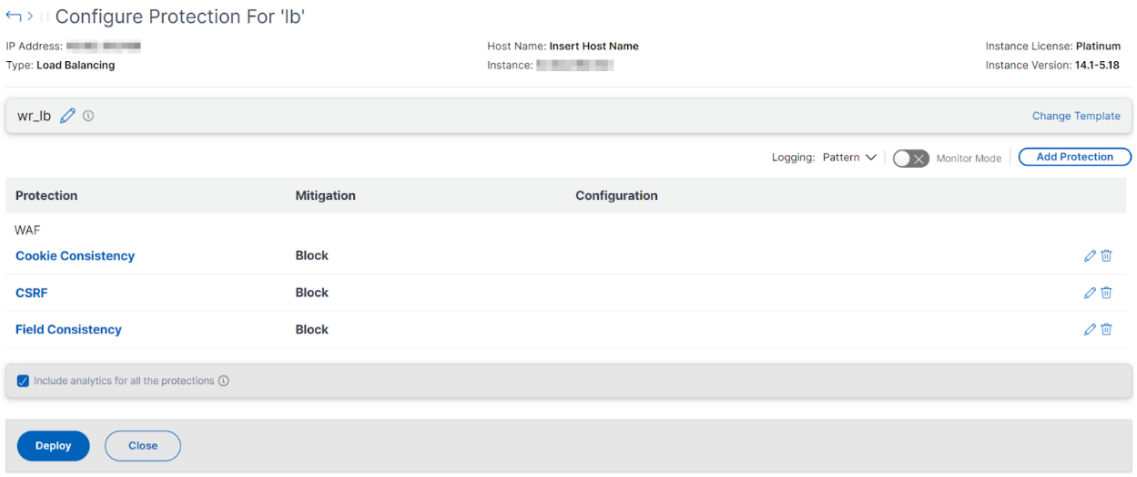
3. WAF 扫描设置配置已完成。您可以单击“开始扫描”开始扫描过程并等待进度完成。扫描完成后，单击“查看报告”。



4. 在扫描结果页面中，单击“查看建议”。



5. 查看保护措施或编辑/添加任何其他保护，然后单击部署。

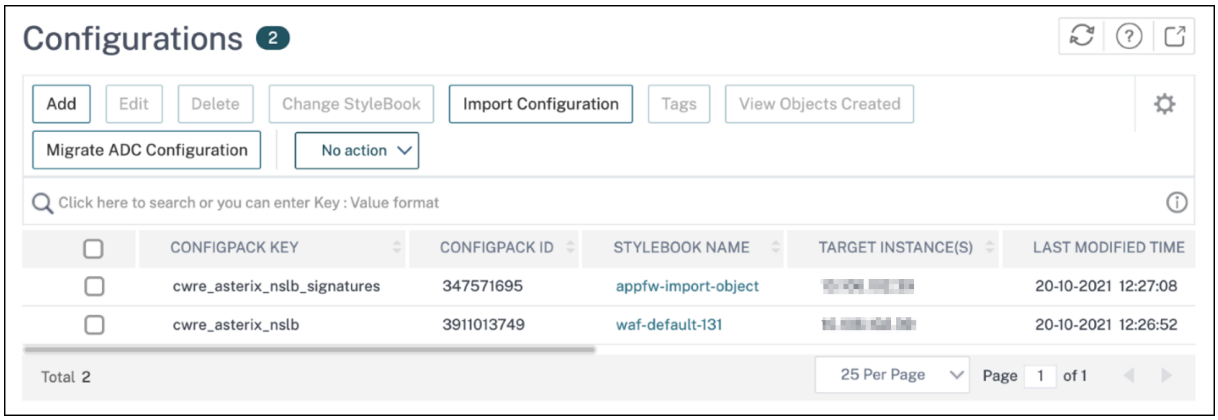


成功应用安全检查后：

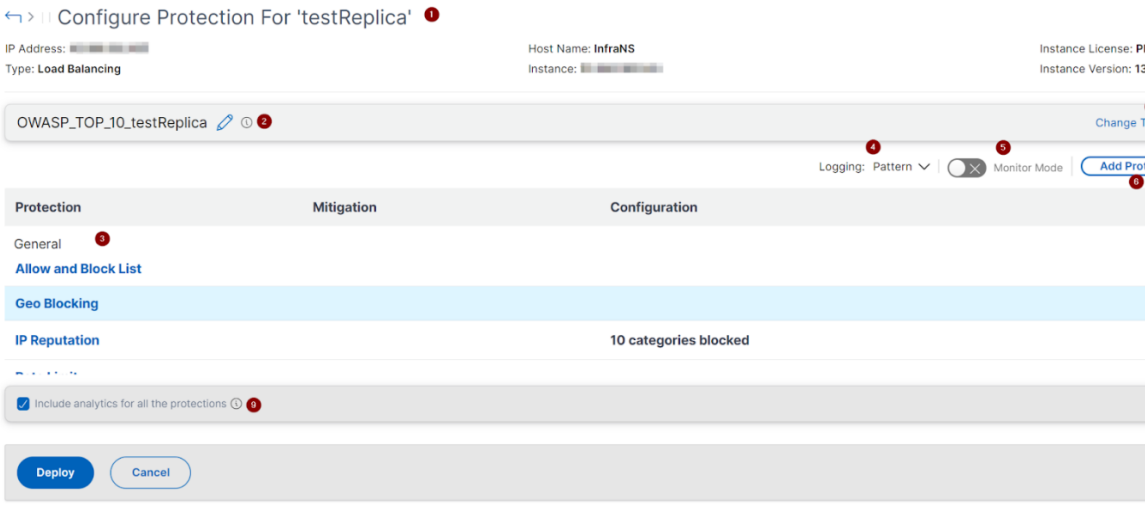
- 该配置通过样书应用到 NetScaler 实例，具体取决于版本。
  - 对于 NetScaler 13.0，`unified-appsec-protection-130` 使用了样书。
  - 对于 NetScaler 13.1，`unified-appsec-protection-131` 使用了样书。
  - 对于 NetScaler 14.1，`unified-appsec-protection-141` 使用了样书。
- `Appfw` 配置文件是在您的 NetScaler 上创建的，并使用 `policylabel` 绑定到应用程序。
- 如果已经应用了建议的签名，则签名将绑定到 appfw 配置文件。

> 注意
>
> NetScaler 13.0 41.28 或更高版本支持安全检查。

您可以通过导航到 应用程序 **>** 配置 **>** 配置包来验证是否通过默认样书应用了 **WAF** 配置文件和签名。



选择和自定义保护



OWASP 前 **10** 名

1 -提供有关应用程序的信息，例如 IP 地址、虚拟服务器类型、许可证类型、配置应用程序的实例等。

2 -显示选定的模板。您可以根据自己的选择对其进行重命名。

3 -显示保护。有些保护措施需要额外的信息。

4 -显示详细日志类型。您可以选择以下选项：

- 模式。仅记录违规模式。
- 模式有效载荷。记录违规模式和 150 字节的额外 JSON 负载。
- 图案、有效载荷、标题。记录违规模式、150 字节的额外 JSON 负载和 HTTP 标头信息。

5 -允许您启用监视模式。如果启用监视模式，则仅记录流量，不会激活缓解措施。

6 -使您能够添加更多保护。单击“添加保护”，然后查看要添加的保护。

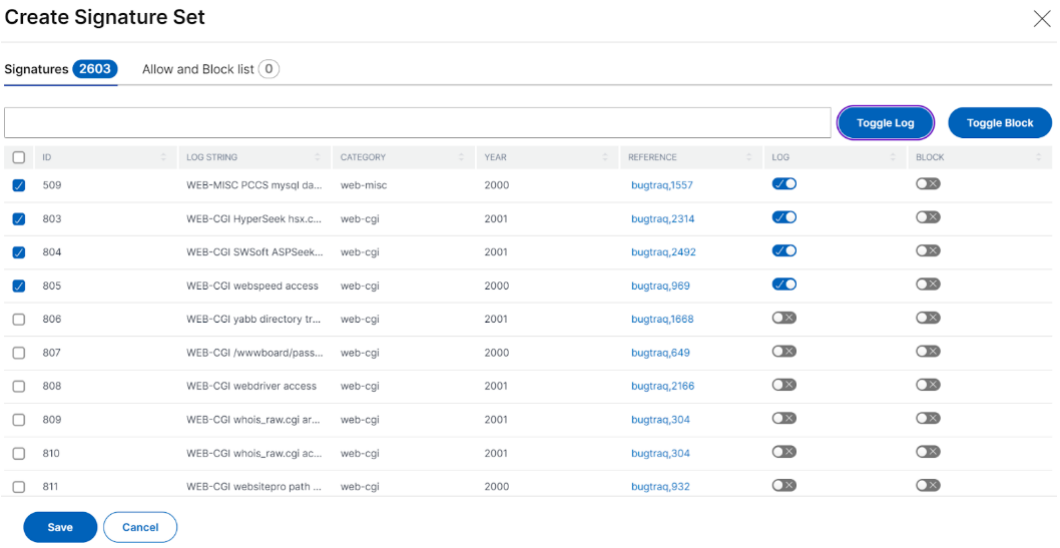
7 -允许您使用“更改模板”选项选择新模板。

8 -允许您编辑或删除保护。

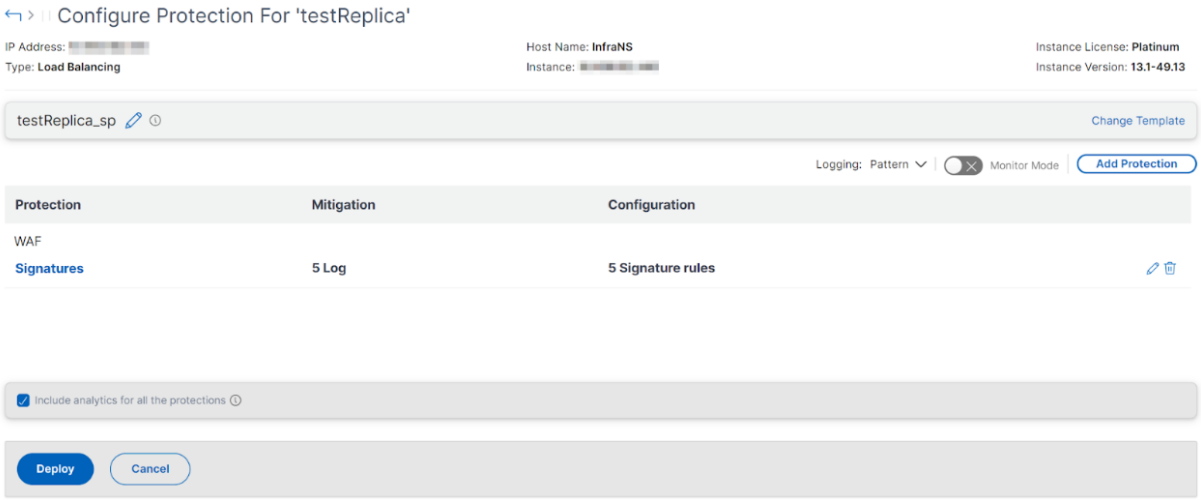
9 -启用对您选择的保护措施的分析。此选项默认处于选中状态。您可以在“安全”**>**“安全违规”中查看对已配置保护的分析。

配置保护后，单击“部署”。

CVE 保护　要部署 CVE 保护，请单击“创建 **CVE** 保护”。在“创建签名集”页面中，从列表中选择签名以配置日志或阻止操作，然后单击“保存”。

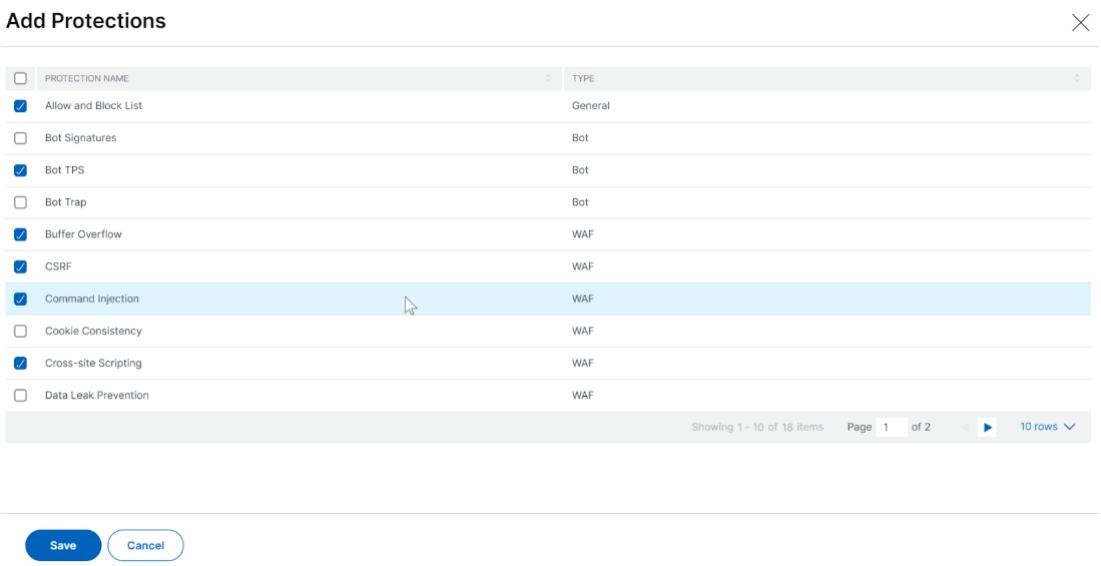


单击“保存”后，可以查看添加到配置页面的签名。



您也可以单击“添加保护”为应用程序添加更多保护。配置所有保护后，单击“部署”。

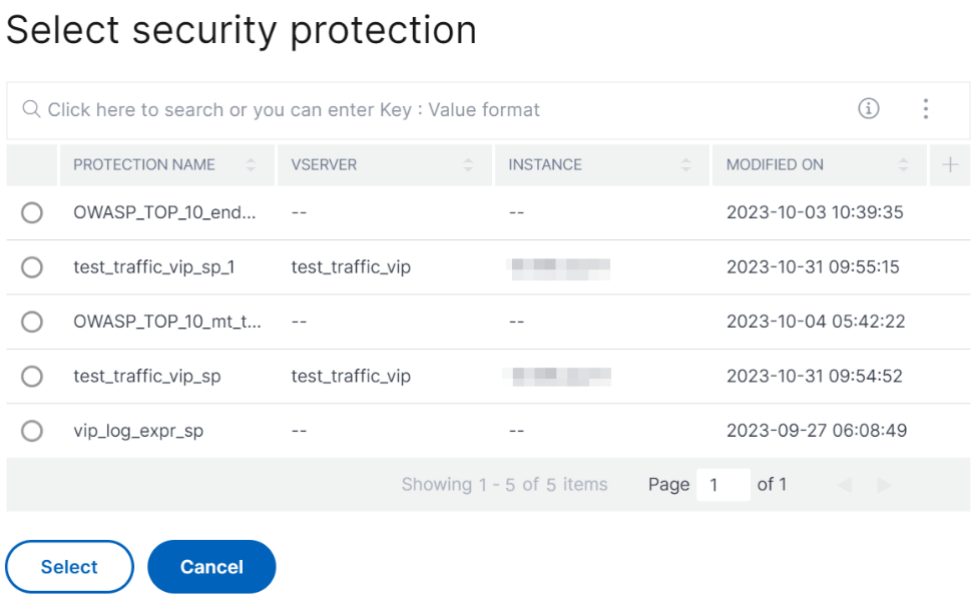
自定义保护　要根据您的要求使用保护进行部署，请单击“创建新保护”。在“添加保护”页面中，选择要部署的保护，然后单击“保存”。



单击“保存”后，查看配置页面中的选定保护，然后单击“部署”。

选择现有保护措施

要将现有保护从一个应用程序部署到另一个应用程序，请从列表中选择现有保护。



选择保护后，现有保护将被克隆并显示在配置页面中。您可以根据需要进行修改，然后单击 **Deploy**。

查看应用程序安全违规详细信息

March 10, 2024

暴露于 Internet 的 Web 应用程序已经变得容易受到严重攻击。NetScaler 控制台使您能够可视化可操作的违规细节，以保护应用程序免受攻击。导航至单窗格解决方案的“安全性”**>**“安全性违规”，以执行以下操作：

- 可视化应用程序，全面了解 WAF 洞察和机器人洞察中相关的威胁细节。有关更多信息，请参阅“统一安全”控制面板。
- 根据 网络、机器人和 **WAF** 等类别访问应用程序安全违规行为。
- 采取纠正措施保护应用程序。

“安全违规”页面有以下选项：

- 应用程序概述—显示具有完全违规、WAF 和机器人违规总数、按国家/地区划分的违规等的应用程序的概述。有关更多信息，请参阅 应用程序概述。
- 所有违规—显示应用程序安全违规详细信息。有关详细信息，请参阅 所有违规。

设置

要查看违规行为，必须确保：

- 开始在应用程序中配置保护和启用分析。有关更多信息，请参阅“统一安全”控制面板。

  如果您已通过样书或直接在 NetScaler 实例上配置了保护，则可以按照以下步骤启用 **WAF** 安全违规和机器人安全违规：

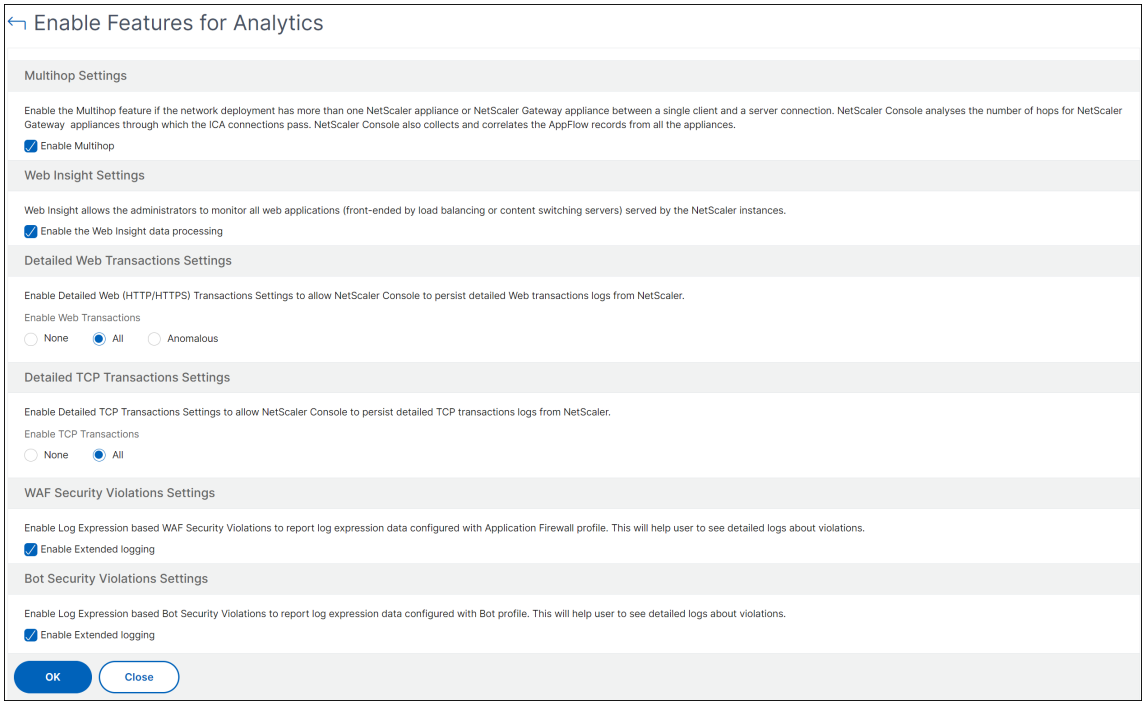
  1. 导航到 基础结构 **>** 实例 **> NetScaler** 并选择实例类型。例如，VPX。
  2. 选择实例，然后从“选择操作”列表中选择“配置分析”。
  3. 选择虚拟服务器，然后单击“启用安全和分析”。
  4. 在“启用分析”窗口中，选择“**WAF** 安全违规”和“机器人安全违规”，然后单击“确定”。
- 配置 详细的 Web 事务设置。
- 如果启用了 指标收集器。有关更多信息，请参阅配置智能应用程序分析。

启用 **Web** 事务设置

1. 导航到“设置”**>**“分析设置”。

   此时将显示“分析设置”页面。

2. 单击启用分析功能。
3. 在 **Web** 事务详细设置下，选择 全部。

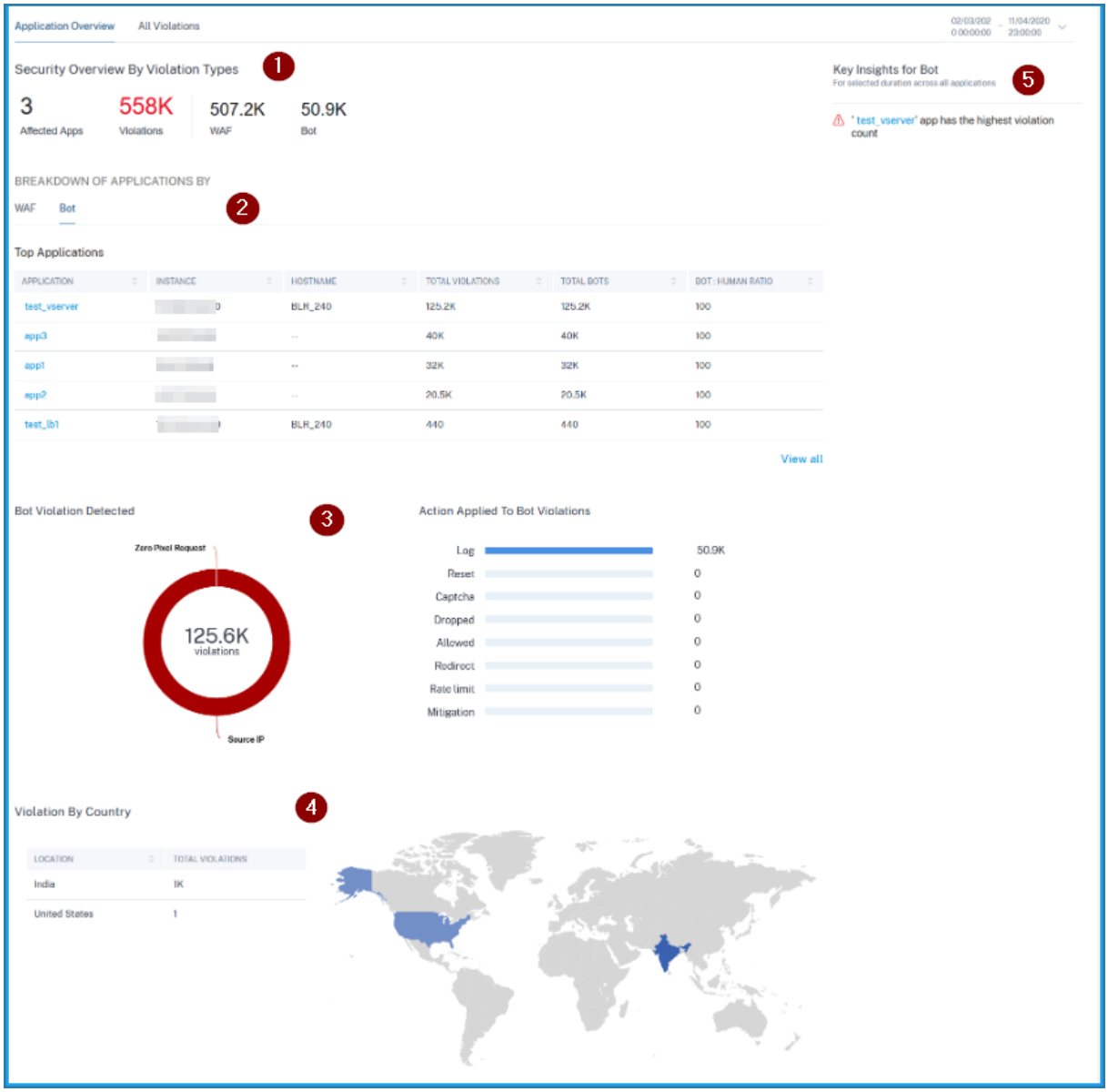


4. 单击确定。

应用程序概述

March 10, 2024

应用程序概述页面显示的应用程序可以完全了解 Security Insight 和机器人洞察中关联的威胁详细信息。您还可以查看诸如总违规、WAF 和机器人违规总数、按国家/地区划分的违规等信息。



1 —显示所选持续时间内受影响的应用程序总数、违规总数、WAF 违规总数以及机器人违规总数。

2 —显示 WAF 和机器人违规的详细信息。单击 **WAF** 和机器人选项卡，根据发生的违规总数查看前 5 个自定义或离散应用程序。单击 查看全部查看所 有应用程序详细信息

3 —根据发生次数和应用的操作显示最严重的违规行为。

4 —显示地理地图视图，提供违规发生地点的可见性。

5 —根据违规提供信息。

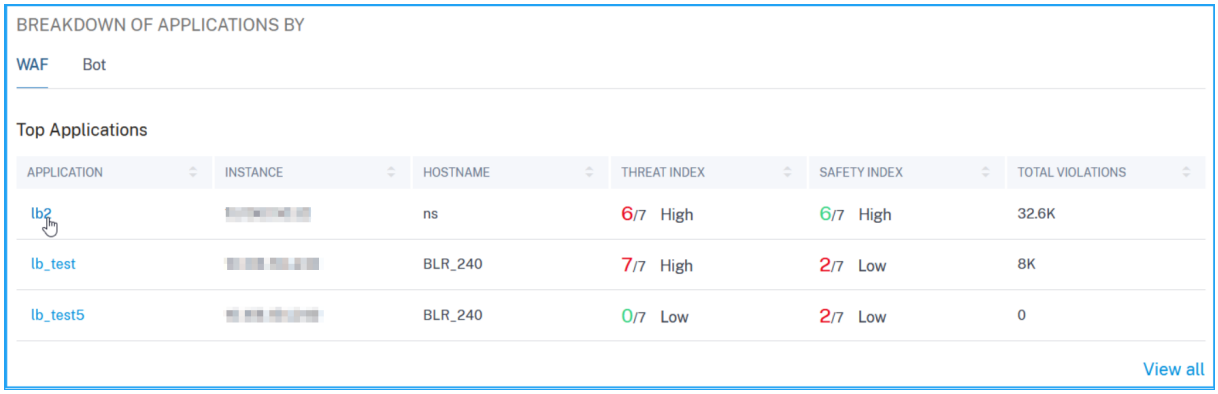
违规类别

WAF	机器人
cookie 劫持	刮刀
推断内容类型 XML	截图创作者
缓冲区溢出	搜索引擎
内容类型	服务代理
Cookie 一致性	站点监视器
CSRF 表单标记	速度测试仪
拒绝 URL	未分类
表单字段一致性	病毒扫描
字段格式	漏洞扫描器
最大上载	DeviceFP 等待超过
推荐人标题	DeviceFP 无效
安全商务	验证码响应无效
安全对象	工具
HTML SQL 注入	验证码尝试超过
起始 URL	有效的验证码响应
跨站点脚本	验证码客户端已静音
XML DoS	验证码等待时间已超过
XML 格式	已超过请求大小限制
XML WSI	已超过费率限制
XML SSL	阻止列表（IP、子网、策略表达式）
XML 附件	允许列表（IP、子网、策略表达式）
XML SOAP 错误	零像素请求
XML 验证	源 IP
其他	主机
IP 信誉	爬虫
HTTP DOS	饲料 Fetcher
TCP 小窗口	链接检查器
违反签名	营销
文件上载类型	地理位置

WAF	机器人
JSON 跨站点脚本	URL
JSON SQL	
JSON DOS	
命令注入	
屏蔽关键字	
JSON 区块关键字	
命令注入语法	

查看 **WAF** 违规详情

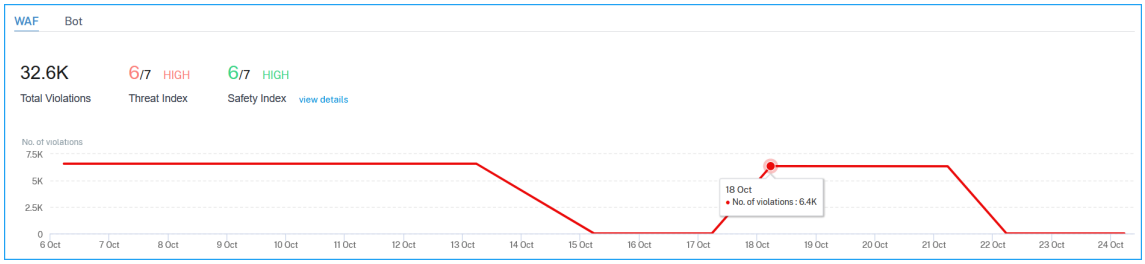
单击排名前几位的应用程序或查看全部选项中的应用程序以查看 WAF 详细信息。



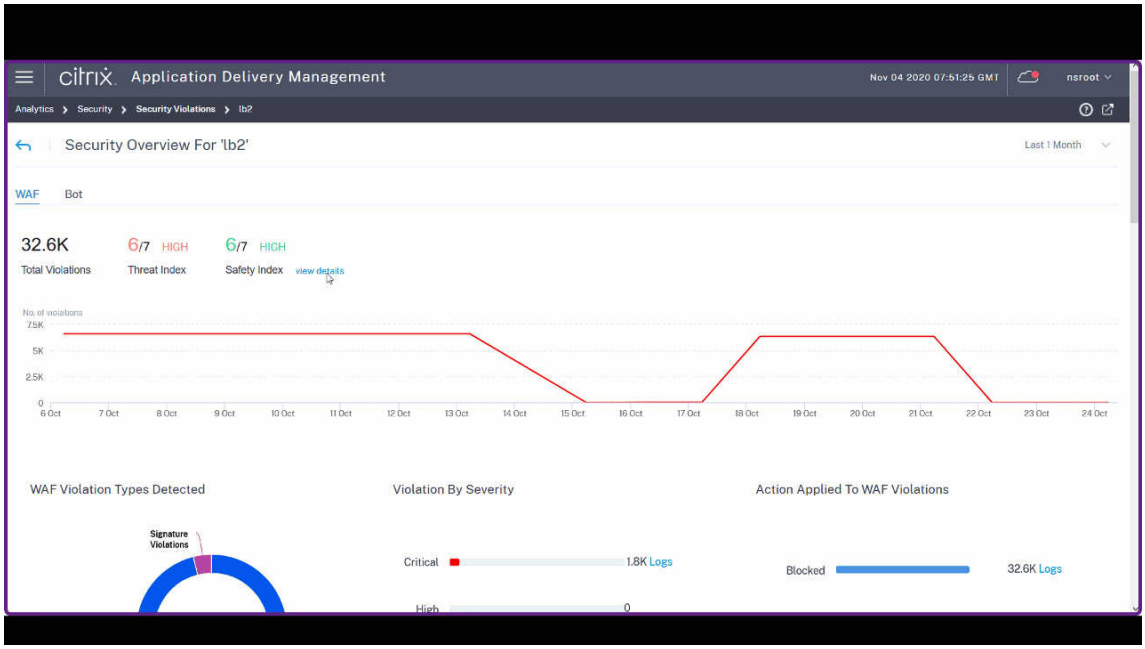
> 注意：
>
> 如果您选择自定义应用程序，则可以在 安全概述 页面中查看合并应用程序的详细信息。从列表中选择一个应用程序以查看所选应用程序的详细信息。

此时将显示所选应用程序的“安全概述”页面。在 **WAF** 下，您可以查看：

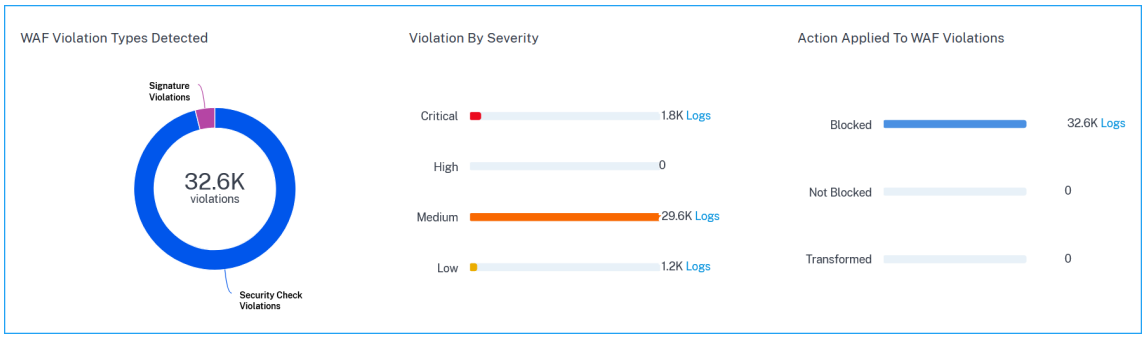
- 指示应用程序的违规总数、威胁指数得分、安全指数得分的图表视图。



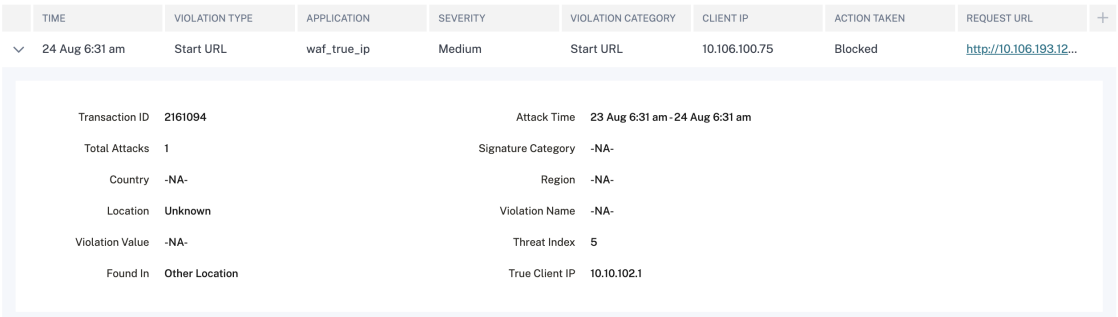
单击 查看详细信息 查看应用程序防火墙和 NetScaler 系统安全配置详细信息。



- 违规基于类型、严重性和应用的操作。



单击 日志 以查看基于严重性或所采取的操作的详细信息。您也可以查看客户端 IP 地址。



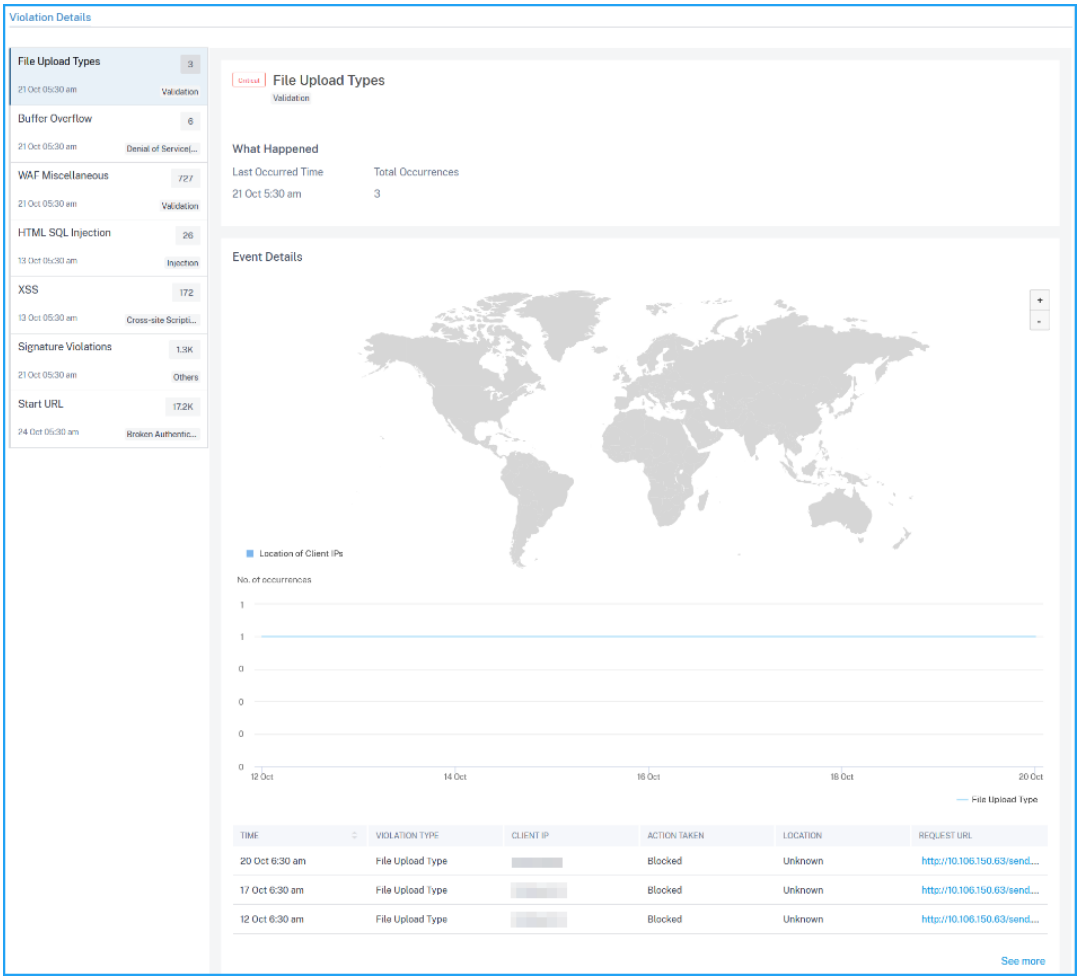
您也可以使用搜索文本框，在其中可以根据需要查看详细信息。当您单击搜索框时，搜索框会为您提供搜索建议列表。

- 受到应用程序影响的违规行为。在 违规详情下，您可以查看受影响的违规详细信息。

> 注意
>
> 对于自定义应用程序，将显示适用于所有应用程序的违规行为。您可以单击列表中的应用程序，查看所选应用程序受影响的违规。

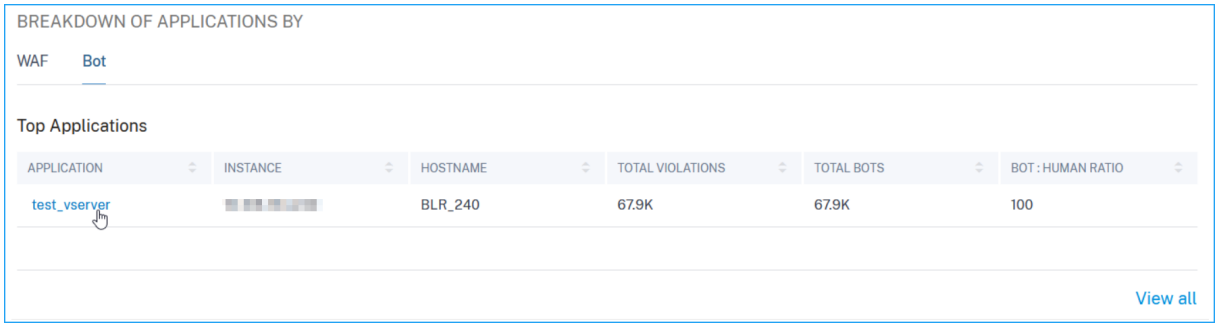
单击每个违规可查看详细信息，例如：

- 发生了什么—表示发生的总数以及上次发生的日期和时间。
- 事件详细信息—显示地理映射，指示客户端 IP 和其他违规详细信息，例如违规类型、客户端 IP、位置等。



查看机器人违规详情

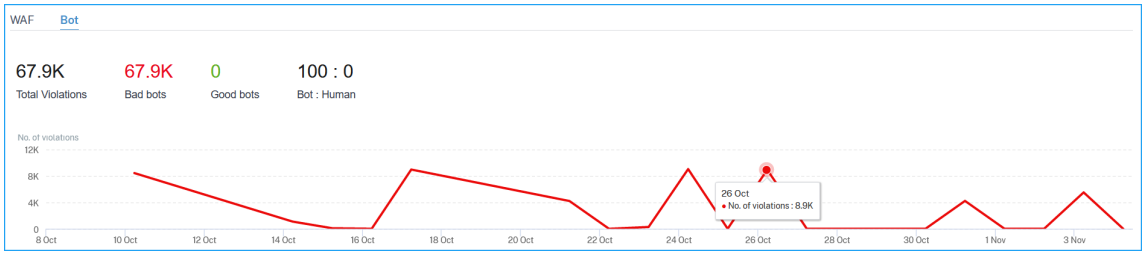
在“机器人”选项卡中，单击“热门应用程序”或“查看全部”选项中的某个应用程序，以查看机器人详细信息。



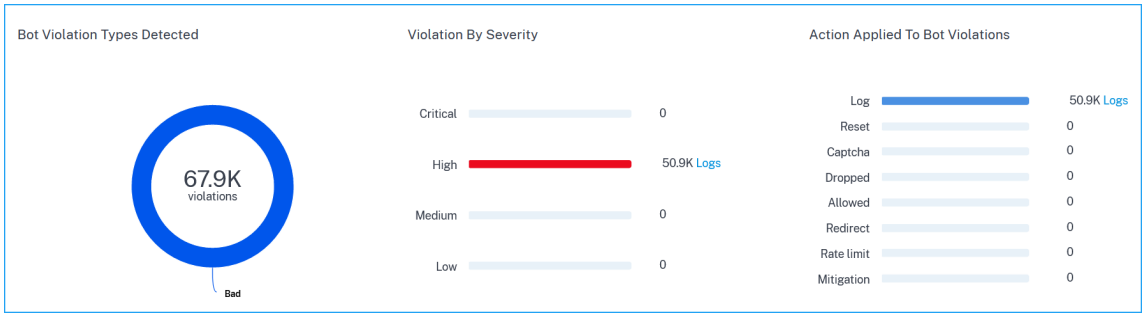
> 注意
>
> 如果您选择自定义应用程序，则可以在 安全概述 页面中查看合并应用程序的详细信息。从列表中选择一个应用程序以查看所选应用程序的详细信息。

此时将显示所选应用程序的“安全概述”页面。在机器人下，您可以查看：

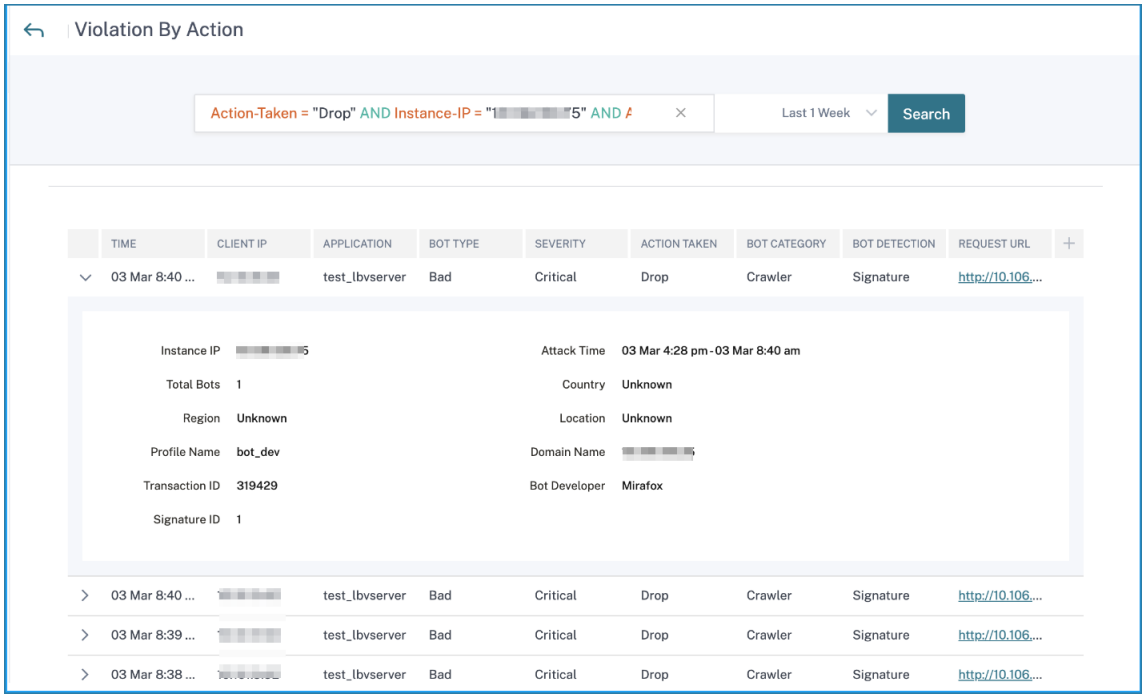
- 显示机器人总数、坏机器人总数、良好机器人总数以及人类用户和访问应用程序的机器人之间的总比率的图表。



- 违规基于机器人类型、严重性和应用的操作。

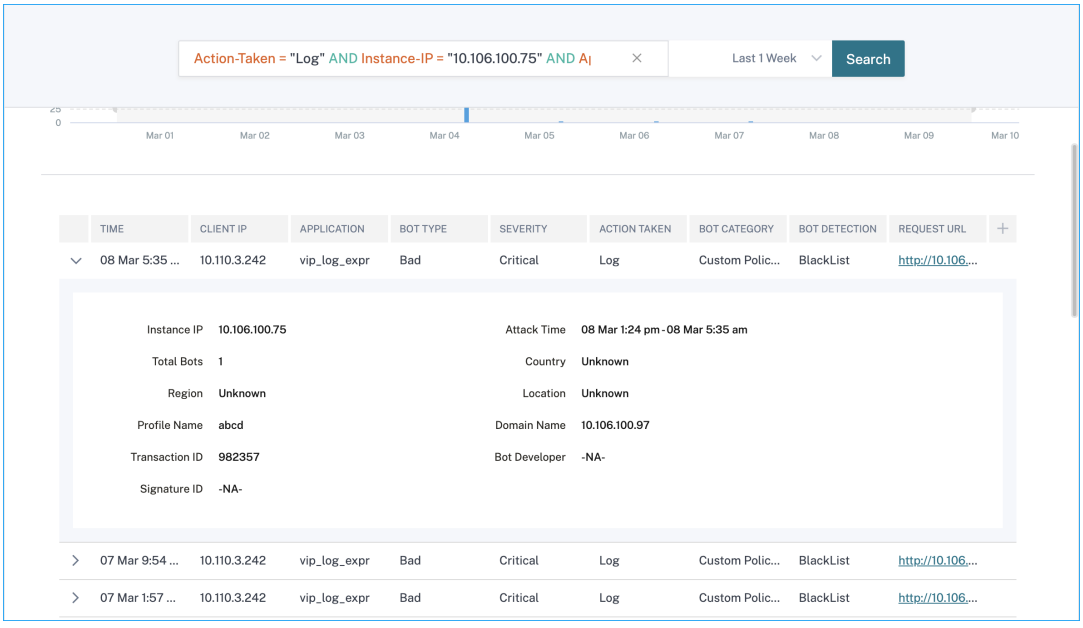


单击 日志 可根据严重性或所采取的操作查看详细信息如果检测到的机器人是签名类型的机器人，您可以查看更多详细信息，例如机器人开发者和签名 ID。通过签名 ID，您可以识别检测到的机器人是好机器人还是坏机器人。



注意：

如果检测到的机器人是除签名机器人以外的任何其他机器人类型，则签名 ID 和机器人开发者将显示为 N/A。



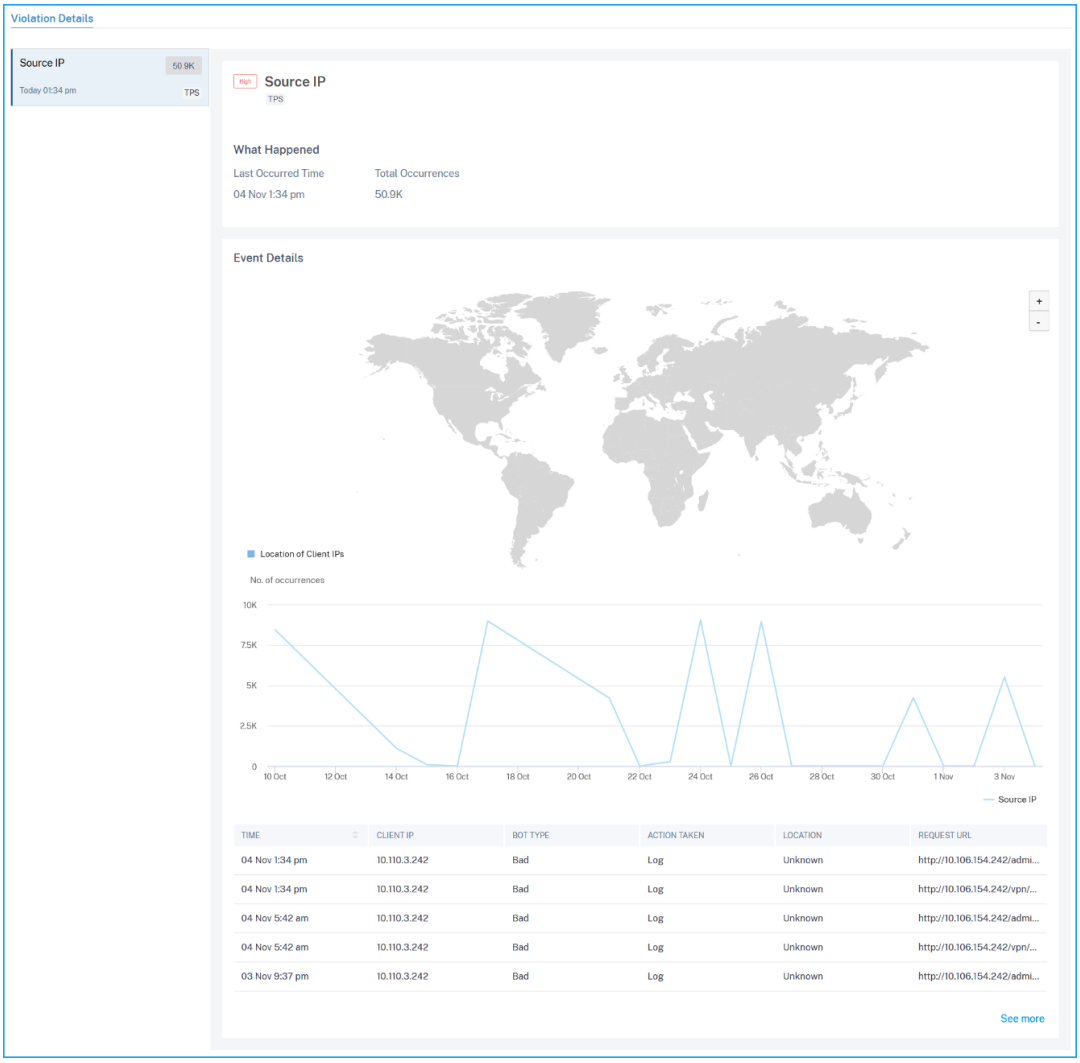
您还可以使用搜索文本框，在其中可以根据需要查看机器人详细信息。当您单击搜索框时，搜索框会为您提供搜索建议列表。

- 受到应用程序影响的违规行为。在 违规详情下，您可以查看受影响的违规详细信息。

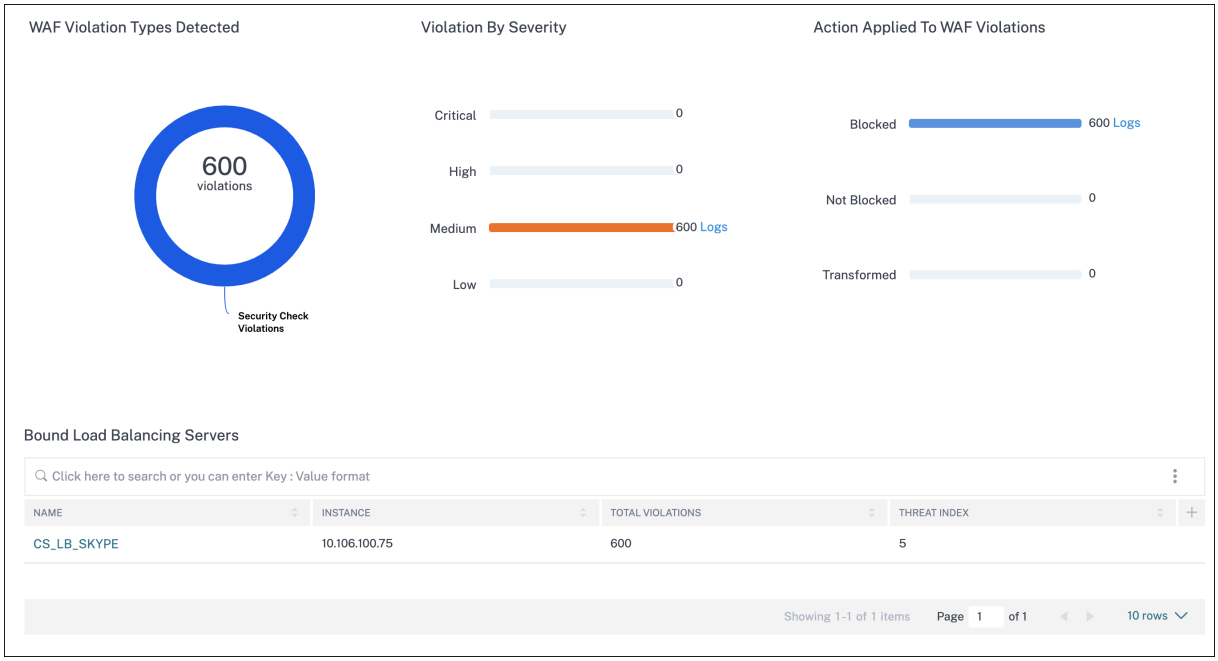
> 注意：
>
> 对于自定义应用程序，将显示适用于所有应用程序的违规行为。您可以单击列表中的应用程序，查看所选应用程序受影响的违规。

单击每个违规可查看详细信息，例如：

- 发生了什么—表示发生的总数以及上次发生的日期和时间。
- 事件详细信息—显示地理映射，指示客户端 IP 和其他违规详细信息，例如违规类型、客户端 IP、位置等。



> 注意：
>
> 在 **WAF** 和机器人下，您可以查看与负载平衡虚拟服务器绑定的内容交换虚拟服务器的分析。单击内容交换虚拟服务器，在“绑定负载平衡服务器”下，可以查看绑定到内容交换虚拟服务器的负载平衡服务器列表。



查看事件历史记录

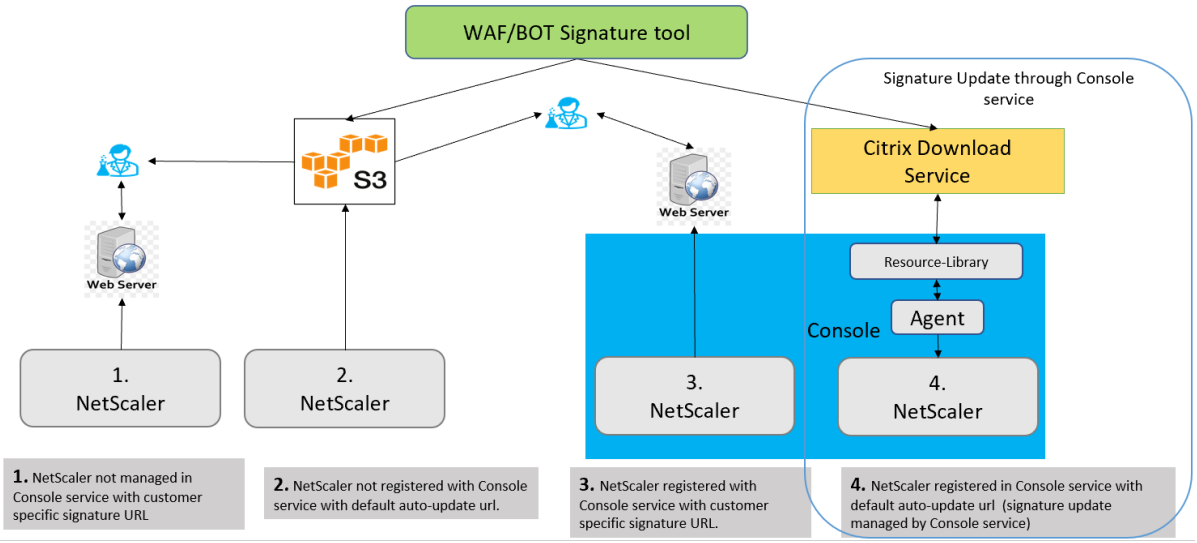
在以下情况下，您可以在“事件”中查看签名更新：

- 在 NetScaler 实例中添加了新签名。
- 在 NetScaler 实例中更新现有签名。

签名自动更新

NetScaler 控制台会自动检查新的签名更新并应用于托管的 NetScaler 实例。

下图显示了如何从 AWS 云检索签名、在 NetScaler 上更新签名以及如何在 NetScaler 控制台上查看签名更新摘要。



所有违规

March 10, 2024

所有违规页面根据网络、**WAF** 和机器人类别显示应用程序安全违规详细信息。要在 NetScaler 控制台中查看安全违规行为，请确保启用了所有必需的设置。有关更多信息，请参阅 设置中提供的程序。

违规类别

使用 NetScaler 控制台，您可以查看以下违规行为。在 违规详细信息下，您可以单击每个违规选项卡以查看违规详细信息。

网络	WAF	机器人
HTTP 慢洛里斯	推断内容类型 XML	刮刀
DNS 慢洛里斯	缓冲区溢出	截图创作者
HTTP 慢速发布	内容类型	搜索引擎
NXDomain 淹没攻击	Cookie 一致性	服务代理
HTTP 不同步攻击	CSRF 表单标记	站点监视器
Bleichenbacher 攻击	拒绝 URL	速度测试仪
Segment smack 攻击	表单字段一致性	工具
SYN 淹没攻击	字段格式	未分类

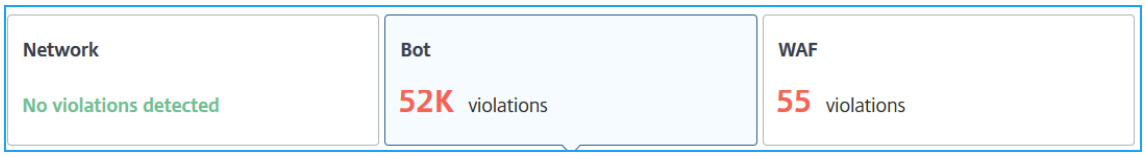
网络	WAF	机器人
小窗口攻击	推荐人标题	病毒扫描
		跨站点脚本
		XML DoS
		XML 格式
		XML WSI
		XML SSL
		XML 附件
		XML SOAP 错误
		XML 验证
		其他
		IP 信誉
		HTTP DOS
		TCP 小窗口
		违反签名
		文件上载类型
		JSON 跨站点脚本
		JSON SQL
		JSON DOS
		命令注入
	cookie 劫持	饲料 Fetcher
	屏蔽关键字	链接检查器
	JSON 区块关键字	营销
		安全商务
		安全对象
		HTML SQL 注入
		起始 URL
	命令注入语法	
	JSON SQL 注入语法	

安全违规控制板

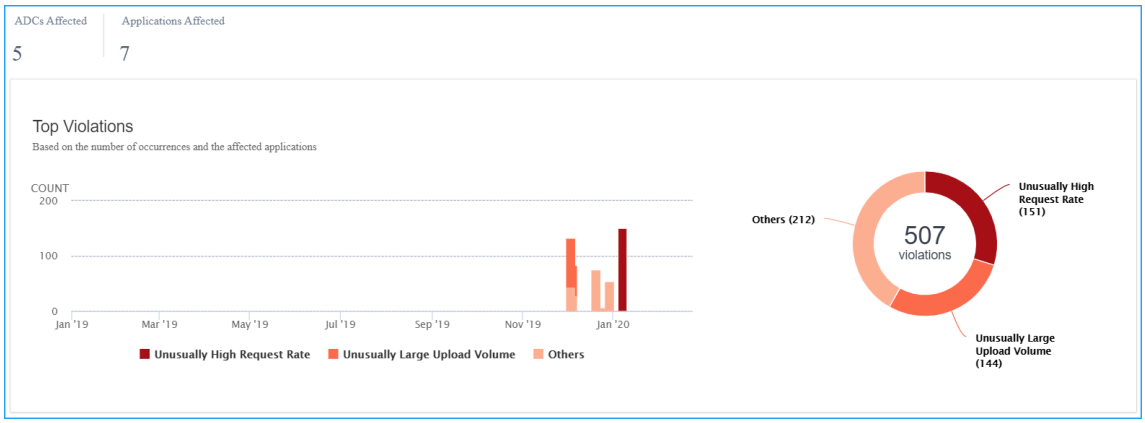
在安全违规控制面板中，您可以查看：

- 所有 NetScaler 实例和应用程序中都发生了违规行为。根据选定的时间持续时间显示违规总数。

- 每个类别下的侵权行为总数。



- 受影响的 NetScaler 实例总数、受影响的应用总数，以及基于总发生次数和受影响应用的最大违规行为。



违规详细信息

对于每种违规行为，NetScaler 控制台都会在特定时间段内监视行为，并检测违规行为是否存在异常行为。单击每个选项卡以查看违规详细信息。您可以查看详细信息，例如：

- 总发生次数、上次发生次数和受影响的应用程序总数
- 在“事件详细信息”下，您可以查看：
  - 受影响的应用程序。如果两个或多个应用程序受到违规影响，您也可以从列表中选择应用程序。
  - 指示违规的图形。
  - 建议您对问题进行 故障排除的建议操作。
  - 其他违规详细信息，例如暴力发生时间和检测信息。

API 安全性

January 29, 2024

API 或应用程序编程接口是一组规则、协议和工具，允许不同的软件应用程序或系统相互通信。API 通过强制执行访问控制、身份验证和加密，确保只有授权实体才能安全地访问和传输机密信息，在保护敏感数据方面发挥着重要作用。

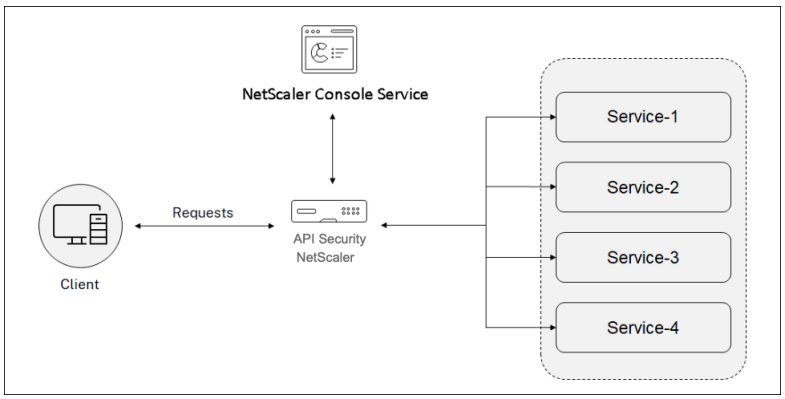
API 可用作移动和 Web 应用程序的后端框架。因此，保护它们传输的敏感数据至关重要。API 安全性是指防止或缓解针对 API 的攻击的做法。

在 API 安全性中，网关充当向 API 端点发出的所有请求的入口点。此外，还可确保安全可靠地访问系统中的所有 API 端点和微服务。

要保护您的 API，请执行以下步骤：

- 创建或上载 API 定义
- 部署 API 实例
- 将策略添加到 API 部署

下图描述了 NetScaler 控制台中的 API 安全如何接收客户端请求并发送来自后端 API 服务的响应：



> 注意：
>
> 在 NetScaler 控制台中，拥有高级或高级许可的用户可以使用此功能。

API 安全性的好处

API 安全性为您提供了以下好处：

- 保护您的 **API** 端点：API 安全性增加了安全层，它可以保护您的 API 端点和后端 API 服务器免受攻击，例如：
  - 缓冲区溢出
  - SQL 注入
  - 跨站点脚本
  - 拒绝服务 (Dos)

- 监视和改进 **API** 性能：API 安全性提供 SSL 卸载、身份验证、授权、速率限制等服务。这些服务提高了 API 性能及其可用性。

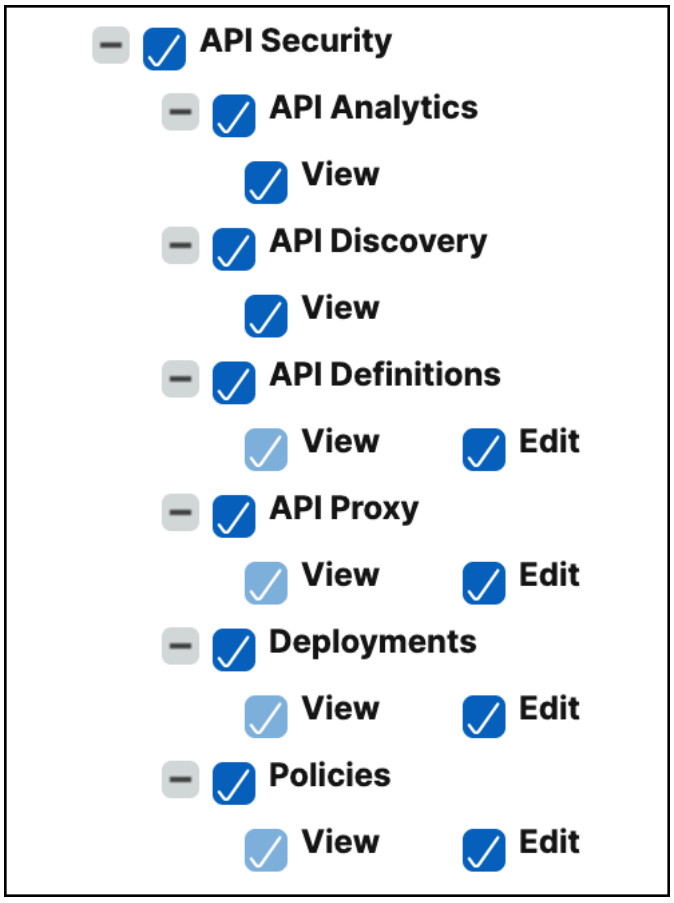
  API 分析为您提供 API 性能指标和 API 端点所面临的威胁的可见性。有关更多信息，请参阅 查看 API 分析。

- 管理 **API** 流量：API 安全性抽象了您的后端 API 基础设施的复杂性。
- 发现 **API** 端点：API 安全性会发现您组织中的 API 端点并添加到 **API** 发现页面。

授予 **API** 安全性配置和管理权限

作为管理员，您可以创建访问策略来授予用户进行 API 安全性配置和管理的权限。用户权限可以是查看、添加、编辑和删除。执行以下操作以授予权限：

1. 导航到“设置” **>** “用户和角色” **>** “访问策略”。
2. 单击添加。
3. 在 创建访问策略中，指定策略名称和描述。
4. 在“权限”字段中，展开“应用程序”，然后展开 **API** 安全性。
5. 选择所需的 **API** 安全性页面。然后，选择要授予的权限。



> 重要：
>
> 确保为使用 API 安全性所需的功能授予权限。例如，如果您授予用户访问“部署”页面的权限，则以下功能还需要用户访问权限：
>
> - 样书
> - IPAM
> - 负载平衡（在 网络功能下）
> - 内容切换（在 网络功能下）
> - 设备 API 代理（在 **API** 下）

有关访问策略的更多信息，请参见 在 NetScaler 控制台上配置访问策略。

WAF 学习

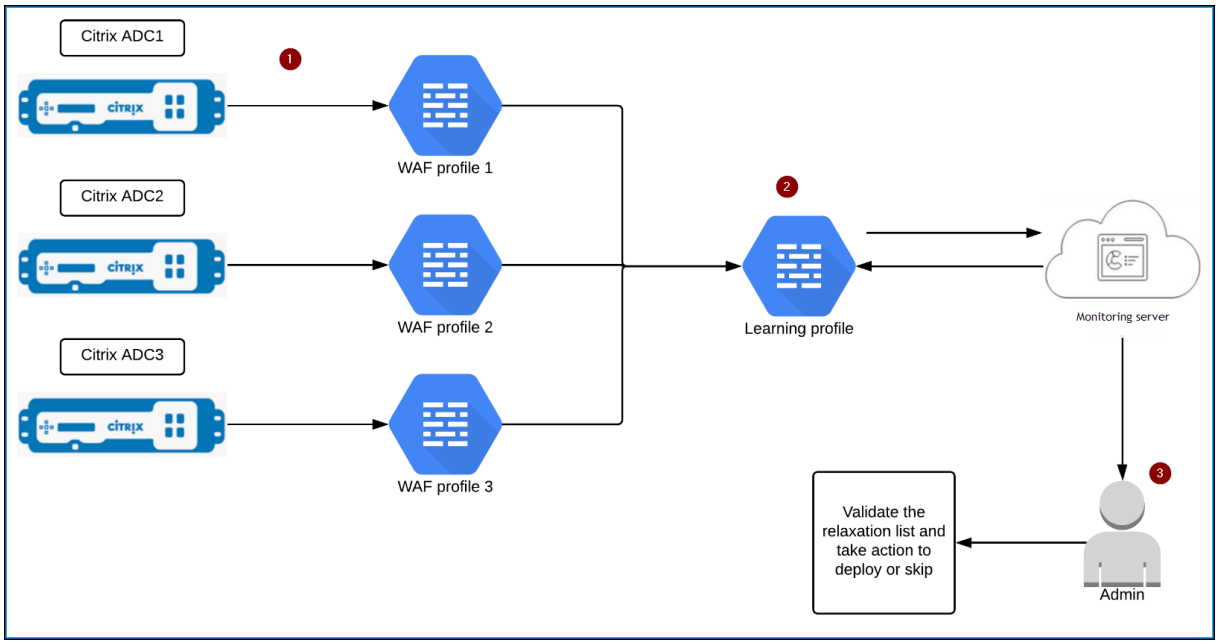
January 29, 2024

NetScaler Web App Firewall (WAF) 可保护您的 Web 应用程序免受 SQL 注入和跨站点脚本等恶意攻击。为了防止数据泄露并提供适当的安全保护，您必须监视流量是否存在威胁以及有关攻击的实时可操作数据。有时，报告的攻击可能是误报，需要作为例外情况提供。

NetScaler 控制台上的学习引擎是一个重复的模式过滤器，它使 WAF 能够学习您的 Web 应用程序的行为（正常活动）。根据监视，引擎会为应用于 HTTP 通信的每个安全检查生成建议的规则或例外列表。

使用学习引擎部署放松规则比在必要时手动部署放松规则要容易得多。

下图说明了有关 NetScaler 控制台中 WAF 学习工作原理的高级信息：



1 —带有其 WAF 配置文件的 NetScaler 实例

2—在 NetScaler 控制台中配置学习配置文件，添加 WAF 配置文件，然后选择自动部署或手动部署放松规则

3—管理员可以在 NetScaler 控制台中验证放松规则，然后决定部署还是跳过

入门

要部署学习功能，您必须：

- 在 NetScaler 实例中启用集中学习。在 NetScaler 实例中运行以下命令：

  ```
  set appfw settings -centralizedLearning ON
  ```

- 确保 NetScaler 实例版本为 **13.0-76.6** 或更高版本。
- 在 NetScaler 设备上配置 Web App Firewall 配置文件（一组安全设置）。有关更多信息，请参阅 创建 Web App Firewall 配置文件。

启用集中式学习并配置 WAF 配置文件后，NetScaler 控制台会为配置的安全检查生成异常（放宽）列表。作为管理员，您可以查看 NetScaler 控制台中的例外列表，然后决定部署还是跳过。

使用 NetScaler 控制台中的 WAF 学习功能，您可以：

- 使用以下安全检查配置学习资料：
  - 起始 URL
  - Cookie 一致性
  - 信用卡

    > 注意
    >
    > 要进行信用卡安全检查，必须在 NetScaler 实例中配置 `doSecureCreditCardLogging`，并确保设置处于关闭状态。

  - 内容类型
  - 表单字段一致性
  - 字段格式
  - CSRF 表单标记
  - HTML 跨站点脚本
  - HTML SQL 注入

> 注意
>
> 要进行 HTML SQL 注入检查，必须在 NetScaler 实例中配置 `set -sqlinjectionTransformSpecial ON` 和 `set -sqlinjectiontype sqlspclcharorkeywords`。

- HTML 命令注入

> 注意
>
> 仅在 NetScaler 实例 13.0-72.12 或更高版本中支持。

- JSON SQL

> 注意
>
> 仅在 NetScaler 实例 13.1-14.10 或更高版本中支持。

- JSON 命令注入

> 注意
>
> 仅在 NetScaler 实例 13.1-14.10 或更高版本中支持。

- JSON XSS

> 注意
>
> 仅在 NetScaler 实例 13.1-14.10 或更高版本中支持。

- 在 NetScaler 控制台中查看放松规则，然后决定采取必要的措施（部署或跳过）
- 通过电子邮件、slack 和 ServiceNow 获取通知
- 使用“操作摘要”页面查看放松详情

要在 NetScaler 控制台中使用 WAF 学习，请执行以下操作：

1. 配置学习配置文件
2. 管理放松规则
3. 使用 WAF 学习操作摘要页面

WAF 建议

January 29, 2024

NetScaler Web App Firewall (WAF) 配置文件和 WAF 签名可保护您的 Web 应用程序免受恶意攻击。WAF 签名提供特定的、可配置的规则，以简化保护您的网站免受已知攻击的任务。签名表示一种模式，该模式是对操作系统、Web 服务器、网站、基于 XML 的 Web 服务或其他资源的已知攻击的组成部分。要使用签名保护应用程序，必须查看规则，启用并配置要应用的规则。

同样，为了防止数据泄露并在应用程序中提供适当的安全保护，您必须创建带有安全检查的 WAF 配置文件。当您在 NetScaler 实例中创建 WAF 配置文件时，流量可能会：

- 使用上述安全检查生成
- 未通过上述安全检查生成

该实例可能正在受到其他攻击，但您可能没有在 WAF 配置文件中启用该安全检查。

作为管理员，您必须了解如何启用正确的签名并创建正确的 WAF 配置文件来保护 Web 应用程序。在某些情况下，识别正确的签名和 WAF 配置文件可能是一项艰巨的任务。

NetScaler 控制台 WAF 建议会扫描应用程序中的漏洞并生成以下建议：

- WAF 配置文件
- WAF 签名

有关更多信息，请参阅 WAF 配置文件 和 WAF 签名。

WAF 建议数据库会频繁更新，以包含任何新漏洞。您可以扫描，然后选择启用所需的建议。您可以启用所有签名和安全检查，但这可能会导致误报并影响 NetScaler 实例性能。因此，建议仅选择所需的安全检查和签名。WAF 建议引擎还会自动检测必须为应用程序启用哪些签名和安全检查。

> 注意
>
> NetScaler 实例 必须是 **13.0 41.28** 或更高版本（用于安全检查）和 **13.0** 或 更高版本（用于签名）。

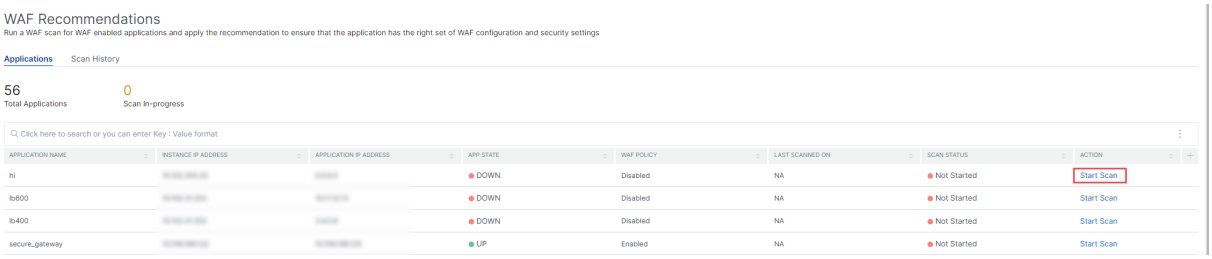
必备条件

应用程序：

- 必须拥有高级许可证。
- 必须是负载平衡虚拟服务器。

配置 **WAF** 扫描设置

在 NetScaler 控制台中，导航 到“安全” **>** “**WAF** 建议”，然后在“应用程序”下单击“开始 扫描”以配置应用程序的 WAF 扫描设置。

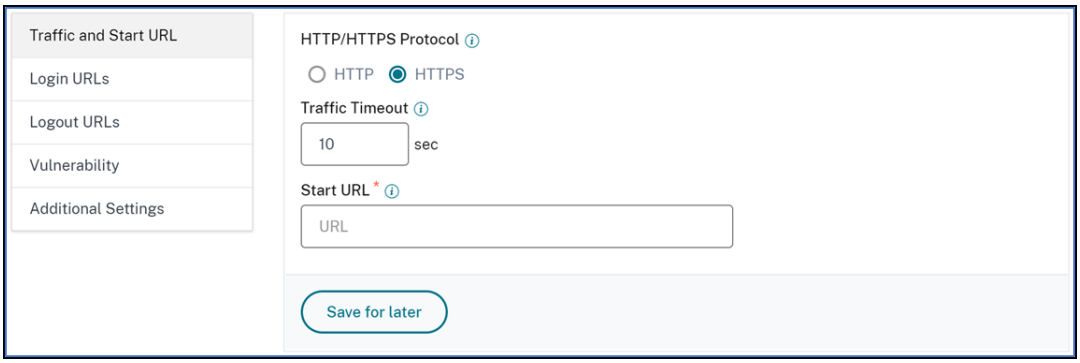


在 WAF 建议页面中：

- 域名—指定与应用程序 VIP 关联的可公开访问/可公开访问的域名。例如：`www.example.com`。

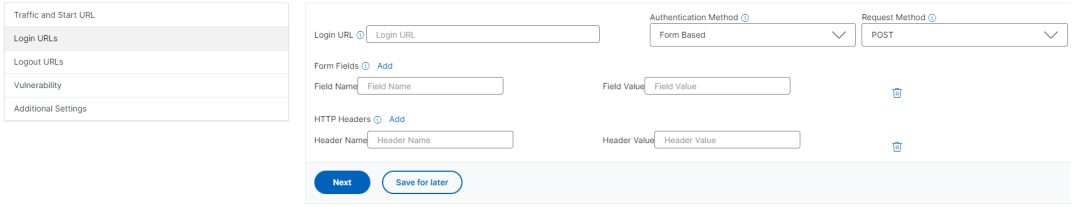
  > 注意
  >
  > 起始 URL、登录 URL 和注销 URL 必须与指定域相匹配。

- 流量和起始网 址-提供应用程序（服务器）的 URL 详细信息。
  - **HTTP/HTTPS** 协议 -选择应用程序的协议。
  - 流量超时 -扫描期间单个请求的等待时间（以秒为单位）。该值必须大于 0。
  - 开始 **URL** —启动扫描的应用程序的主页。例如，`https://www.example.com/home`。URL 必须是有效的 IPv4 地址。如果 IP 地址是私有的，则必须确保可以从 NetScaler 控制台管理 IP 访问私有 IP 地址。

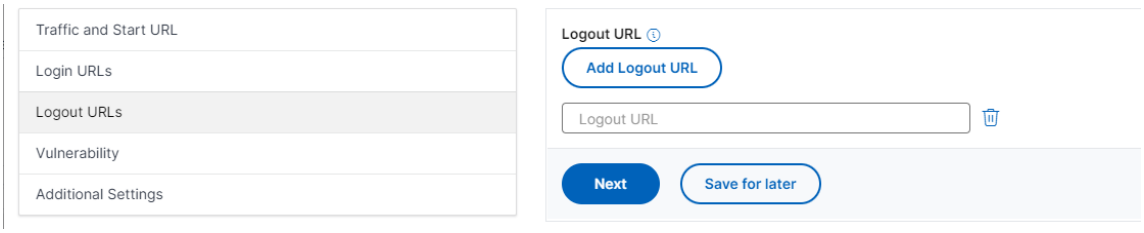


- 登录 **URL** —指定访问应用程序的登录凭据、URL（如果有）。
  - 登录 **UR** L —用于身份验证的登录数据发送到的 URL。在 HTML 中，此 URL 通常被称为操作 URL。
  - 身份验证方法 -为您的应用程序选择支持的身份验证方法（基于表单或基于标题）。
    - 基于表单的身份验证需要使用登录凭据向登录 URL 提交表单。这些凭据必须采用表单字段及其值的形式。然后，应用程序共享用于在扫描期间维护会话的会话 cookie。
    - 基于标头的身份验证需要标头部分中的身份验证标头及其值。身份验证标头必须具有有效值，用于在扫描期间维护会话。表单字段应留空以用于基于标题。
  - 请求方法 -选择向登录 URL 提交表单数据时使用的 HTTP 方法。允许的请求方法是 POST、GET 和 PUT。

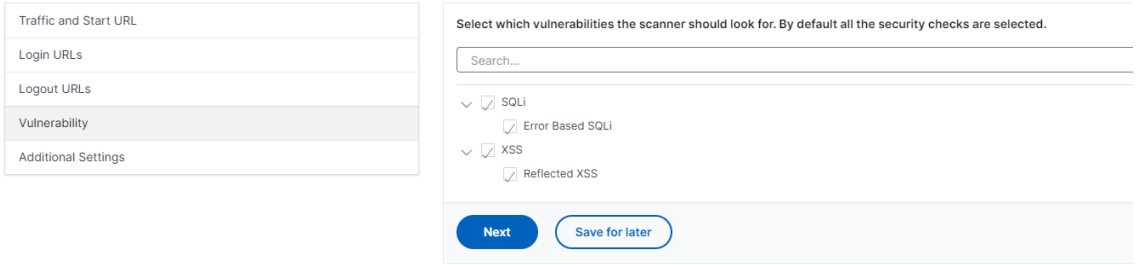
- 表单字段—指定要提交到登录 URL 的表单数据。只有选择基于表单的身份验证时，表单字段才是必填字段。您必须在键值对中指定，其中字段名是“键”，字段值是“值”。确保正确添加登录所需的所有表单字段，包括密码。这些值在存储到数据库之前经过加密。您可以单击“添加”按钮来添加多个表单域。例如，字段名称 -用户名和 字段值 -管理员。
- **HTTP** 标头—成功登录可能需要这些 HTTP 标头。您必须在键值对中指定，其中“标头名称”是键，标头值是值。您可以单击“添加”按钮来添加多个 HTTP 标头。最常用的 HTTP 标头之一是内容类型标头。



- 注销 **URL** —指定访问后终止会话的 URL。例如：`https://www.example.com/customer/logout`。

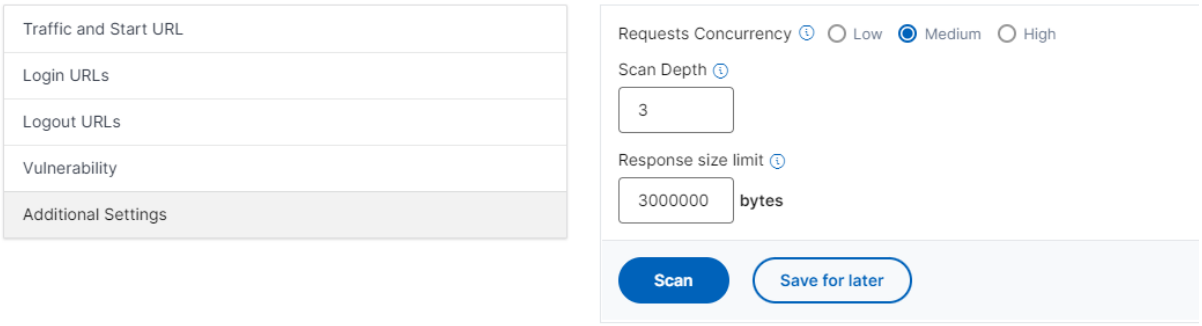


- 漏 洞-选择漏洞供扫描程序检测出来。目前，这是针对 SQL 注入和跨站点脚本冲突执行的。默认情况下，所有违规行为均处于选中状态。选择漏洞后，它会模拟对应用程序的这些攻击，以报告潜在的漏洞。建议启用不在生产环境中的这种检测。还报告了所有其他漏洞，但没有模拟对应用程序的这些攻击。



- 其他设置
  - 请求并发 -并行发送到 Web 应用程序的请求总数。
  - 扫描深 度-必须继续扫描的 Web 应用程序的深度。例如，对于值为 2 的扫描深度，将扫描“开始 URL”和此 URL 中找到的所有链接。必须指定一个大于或等于 1 的值。
  - 响应大小限制 -响应大小的最大限制。不扫描超过上述值的任何响应。建议的限制为 3 MB（300,000 字节）。

WAF 扫描设置配置已完成。您可以单击“扫描”开始扫描过程，也可以单击“保存以供稍后 使用”以保存配置并在以后扫描。



WAF 扫描建议流程

当您开始扫描时，WAF 建议引擎：

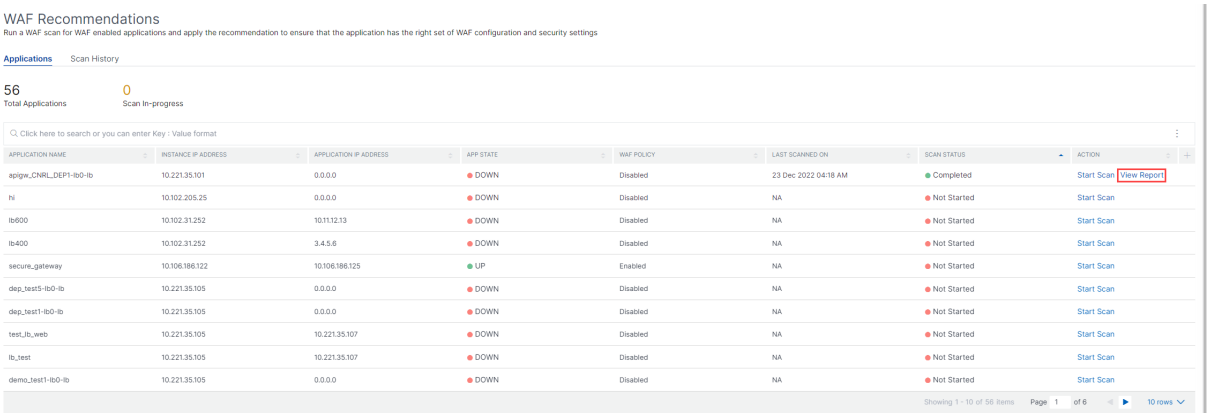
- 通过提供的 URL 扫描提供的 Web 应用程序。
- 检查 Web 应用程序以发现 Web 应用程序使用的技术。
- 模拟 Web 应用程序上的安全攻击以检测潜在漏洞。
- 根据检测到的 Web 技术建议签名。
- 根据发现的漏洞和流量分析建议安全检查。
- 分析 Web 应用程序响应以生成更精细的设置。

支持以下安全检查：

- 缓冲区溢出
- 字段格式
- 信用卡
- Cookie 一致性
- HTML SQL 注入
- HTML 跨站点脚本编写
- 表单字段一致性
- CSRF 表单标记

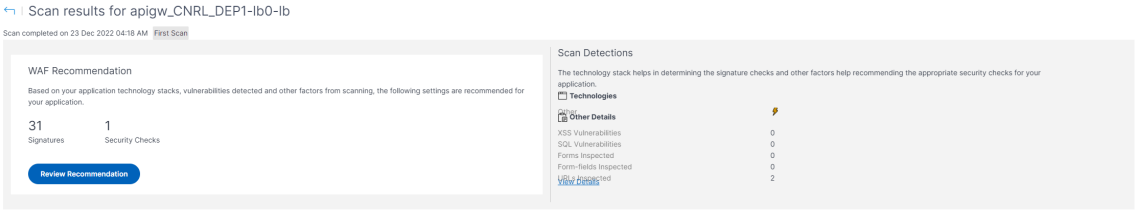
查看扫描报告

扫描完成后，单击“查看报告”以查看结果。



扫描结果提供：

- **WAF** 建议 -使您能够查看为应用程序建议的总签名和安全检查摘要。
- 扫描检测 -使您能够查看在应用程序上执行的技术和违规详细信息等信息的收集。单击“查看详细信息”以查看有关检测的信息以及扫描的其他详细信息。



在 **WAF** 建议下，单击“查看建议”以查看 安全检查 和 签名的详细信息。

建议的安全设置建议对应用程序进行建议的安全检查和签名。您可以编辑列表中的建议，然后单击“查看”或“编辑”以查看详细信息或根据要求编辑更改。“重置为默认值”会重置所有更改并恢复为原始建议。

查看详细信息后，单击“应用建议”。建议是使用样书配置的。必须确保分别应用“安全检查”和“签名”选项卡中的建议。

建议先应用签名，然后再进行安全检查。这会自动将签名绑定到配置文件。

成功应用签名后：

- 该配置通过 `appfw-import-object` 样书应用于 NetScaler 实例。
- 配置了建议的签名文件将导入到 NetScaler 实例中。

> 注意
>
> NetScaler 13.0 或更高版本支持签名。

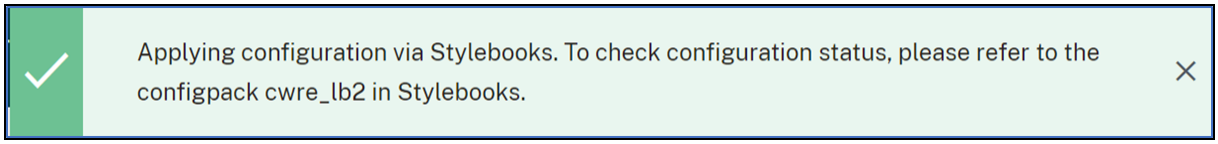
在继续应用 安全检查 建议之前，请导航到 应用程序 > 配置 > 配置包，并确保签名 configpack 已成功创建。

成功应用安全检查后：

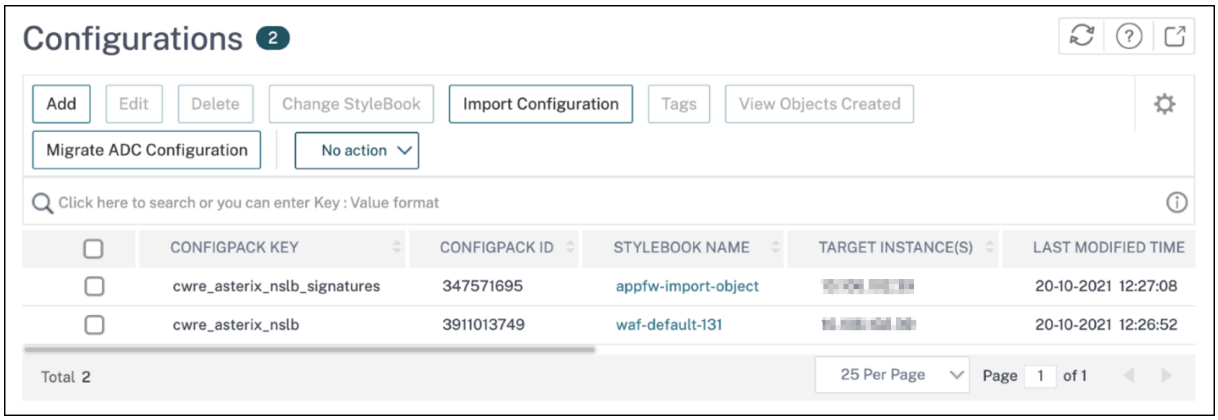
- 该配置通过样书应用于 NetScaler 实例，具体取决于 NetScaler 版本。对于 NetScaler 13.0 ，使用 `waf-default-130` 样书，对于 NetScaler 13.1，使用 `waf-default-131` 样书。
- `Appfw` 配置文件是在您的 NetScaler 上创建的，并使用 `policylabel` 绑定到应用程序。
- 如果已经应用了建议的签名，则签名将绑定到 appfw 配置文件。

> 注意
>
> NetScaler 13.0 41.28 或更高版本支持安全检查。

应用建议（安全检查和签名）后，您可以查看以下确认消息：



您可以通过导航到 应用程序 > 配置 > 配置包来验证是否通过默认样书应用了 **WAF** 配置文件和签名。



Gateway Insight

March 10, 2024

在 NetScaler Gateway 部署中，查看用户访问详细信息对于排查访问失败问题至关重要。作为网络管理员，您希望知道用户何时无法登录 NetScaler Gateway，并且希望了解用户活动和登录失败的原因，但除非用户发送解析请求，否则该信息通常不可用。

通过 Gateway Insight 可以查看所有用户登录 NetScaler Gateway 时遇到的失败，而无论访问模式为何。可以查看所有可用用户列表，以及任何给定时间的活动用户数、活动会话数及所有用户使用的字节数和许可证数。可以查看某个用户的端点分析 (EPA)、身份验证、单点登录 (SSO) 及应用程序启动失败。还可以查看某个用户的活动会话和已终止会话的详细信息。

通过 Gateway Insight 还可以查看虚拟应用程序的应用程序启动失败的原因。这可提高您对任何登录或应用程序启动失败问题进行故障排除的能力。可以查看启动的应用程序数、总会话数和活动会话数、应用程序使用的总字节数和带宽。可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

您可以查看与 NetScaler Gateway 设备关联的所有网关在任何给定时间使用的网关数量、活动会话数、总字节数和带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其登录活动的详细信息。

所有日志消息都存储在 NetScaler 控制台数据库中，因此您可以查看任何时间段的错误详情。还可以查看登录失败摘要，并确定在登录过程的什么阶段发生了失败。

注意事项：

- 以下部署支持 Gateway Insight：
  - Access Gateway
  - Unified Gateway
- NetScaler 控制台的版本和版本必须与 NetScaler Gateway 设备的版本和版本相同或更晚。
- 可以查看具有高级许可证的 NetScaler 实例的一小时 Gateway Insight 报告。查看超过一小时的 Gateway Insight 报告需要高级许可证。

限制：

- 当身份验证方法配置为基于证书的身份验证时，NetScaler Gateway 网关不支持 Gateway Insight。
- 在 HDX Insight“Users”（用户）控制板上只能看到虚拟 ICA 应用程序和桌面的成功用户登录、延迟及应用程序级别详细信息。
- 在双跃点模式下，无法查看第二个 DMZ 中 NetScaler Gateway 设备上的失败。
- 远程桌面协议 (RDP) 桌面访问问题不会报告。
- 未报告 SAML 身份验证的 Gateway Insight 记录。
- 以下身份验证类型支持 Gateway Insight。如果使用其他身份验证类型，您可能会在 Gateway Insight 中看到一些差异。
  - 本地
  - LDAP

- RADIUS
- TACACS
- SAML
- 本机 OTP
- OAuth

启用 **Gateway Insight**

要为您的 NetScaler Gateway 设备启用 Gateway Insight，必须先将 NetScaler Gateway 设备添加到 NetScaler 控制台。然后必须为表示 VPN 应用程序的虚拟服务器启用 AppFlow。有关向 NetScaler 控制台添加设备的信息，请参见添加实例。

> 注意
>
> 要在 NetScaler 控制台中查看端点分析 (EPA) 故障，必须在 NetScaler Gateway 设备上 启用 AppFlow 身份验证、授权和访问控制用户名记录。

在 **NetScaler** 控制台中为虚拟服务器启用 **AppFlow**

1. 导航到 **Settings**（设置）**> Licensing & Analytics Configuration**（许可和分析配置）。
2. 在“虚拟服务器分析摘要”下，单击“配置分析”。
3. 在“所有虚拟服务器”页面中，选择 NetScaler Gateway 虚拟服务器，然后单击“启用安全和分析”。
4. 选择 **Gateway Insight**。
5. 单击保存。

使用 **GUI** 在 **NetScaler Gateway** 设备上启用 **AppFlow** 用户名登录

1. 导航到配置 **>** 系统 **> AppFlow >** 设置，然后单击更改 **AppFlow** 设置。
2. 在“配置 **AppFlow** 设置”屏幕中，选择 **AAA** 用户名，然后单击“确定”。

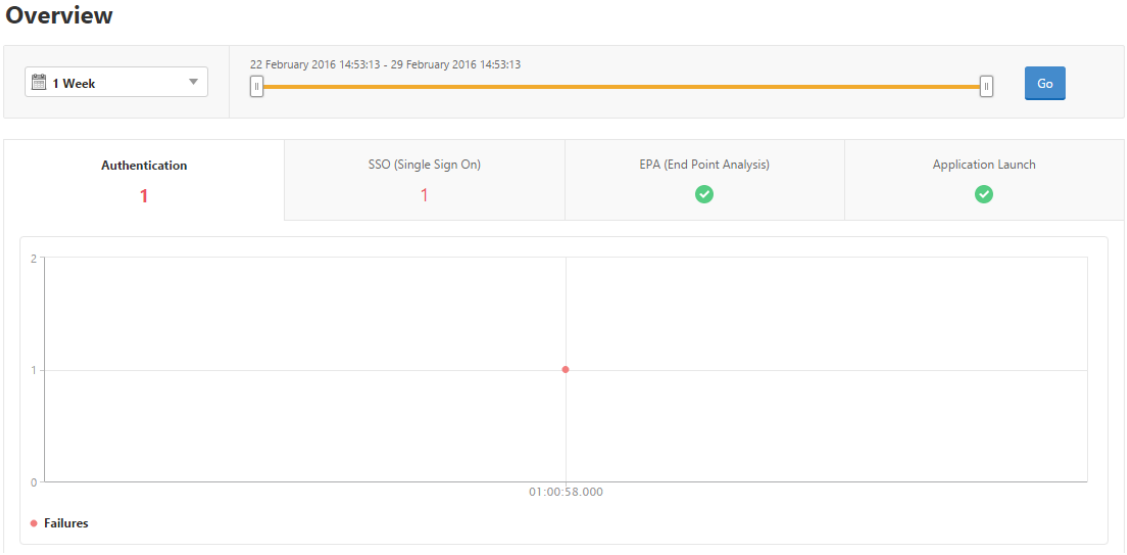
查看 **Gateway Insight** 报告

在 NetScaler 控制台中，您可以查看与 NetScaler Gateway 设备关联的所有用户、应用和网关的报告，还可以查看特定用户、应用或网关的详细信息。在“概 述”部分，您可以查看 EPA、SSO、身份验证和应用程序启动失败。还可以查看用户用于登录的不同会话模式、客户端类型及每小时登录用户数的摘要。

> 注意：
>
> 创建组时，您可以为组分配角色、提供对组的应用程序级别访问权限以及将用户分配给组。NetScaler 控制台分析现在支持基于虚拟 IP 地址的授权。您的用户现在只能看到他们被授权的应用程序（虚拟服务器）的所有见解报告。有关组和向组分配用户的详细信息，请参阅在 NetScaler 控制台上配置组。

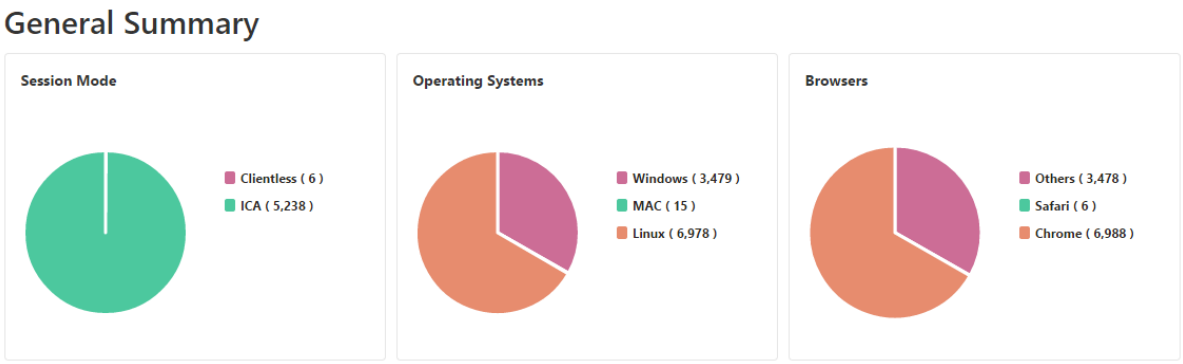
查看 **EPA**、**SSO**、身份验证、授权和应用程序启动失败

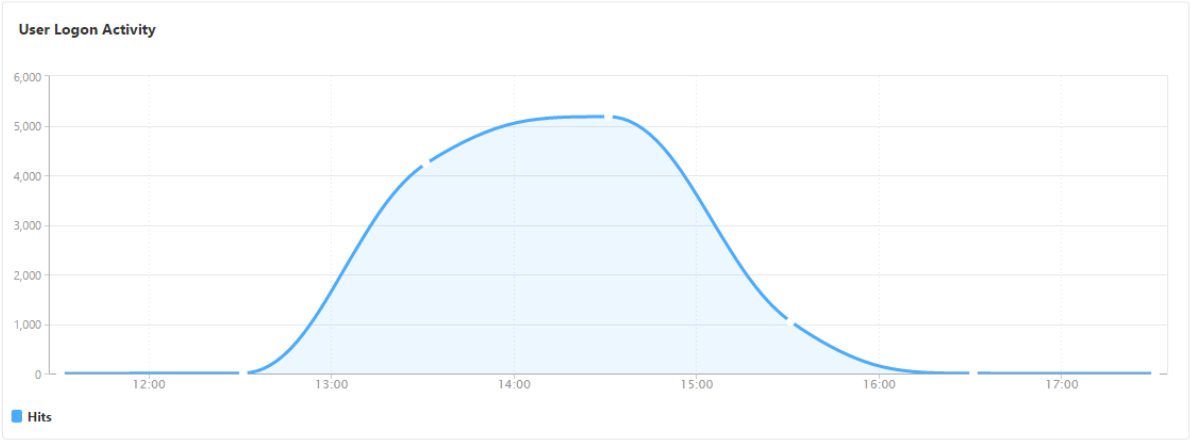
1. 在 NetScaler 控制台中，导航到 **Gateway >** GatewayInsight。
2. 选择要查看用户详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 单击 “EPA (End Point Analysis)”（EPA(端点分析)）、“Authentication”（身份验证）、“Authorization”（授权）、“SSO (Single Sign On)”（SSO(单点登录)）或 “Application Launch”（应用程序启动）选项卡以显示失败详细信息。



查看会话模式、客户端和用户数的摘要

在 NetScaler 控制台中，导航 到 Gateway **> Gateway Insight**，向下滚动查看报告。

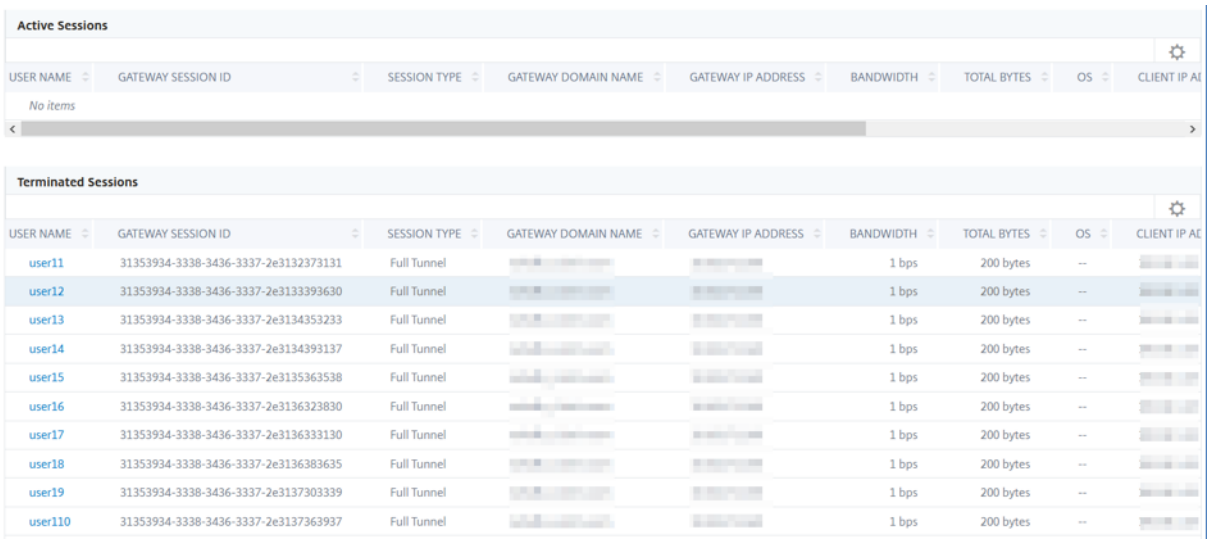




用户

您可以查看与 NetScaler Gateway 设备关联的用户的完整报告。您可以查看用户的 EPA、身份验证、SSO、应用程序启动失败等。

您还可以直观显示所有用户活动和已终止会话的合并视图。



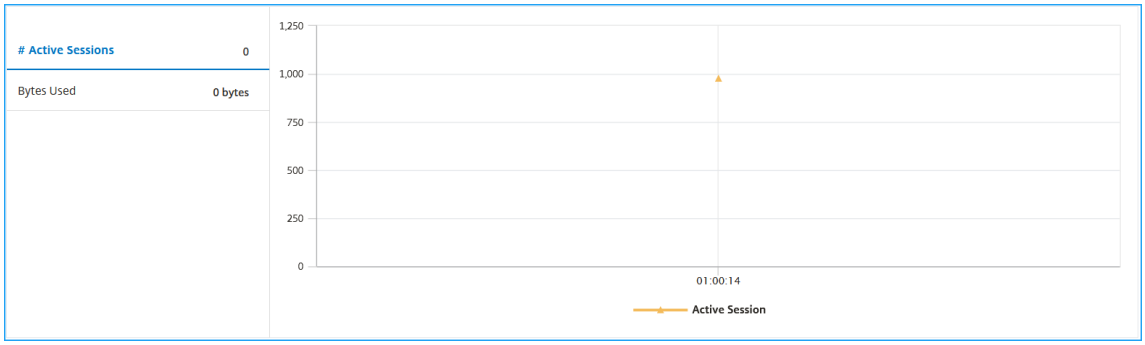
作为管理员，此视图使您能够：

- 在单窗格可视化中查看所有用户详细信息
- 消除选择每个用户以及查看活动和已终止会话的复杂性

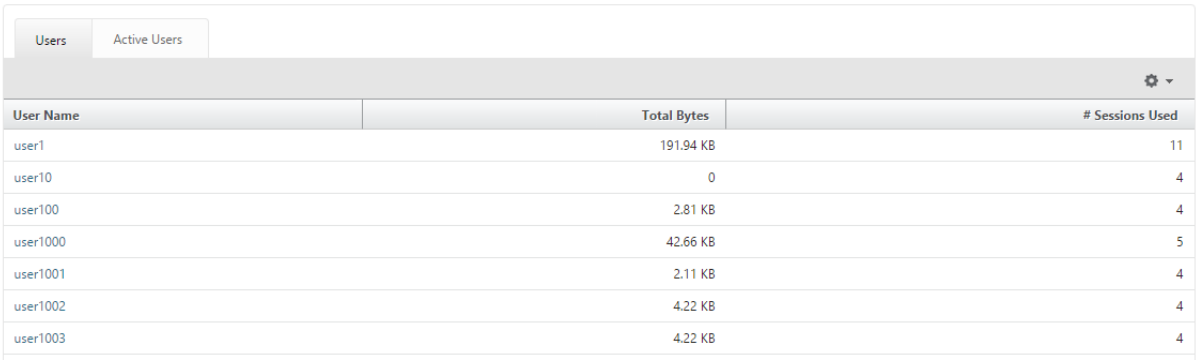
查看用户详情

1. 在 NetScaler 控制台中，导航 到 **Gateway > Gateway Insight >** 用户。
2. 选择要查看用户详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

3. 您可以查看该时段内活动用户的数量、活动会话数和所有用户的字节数。



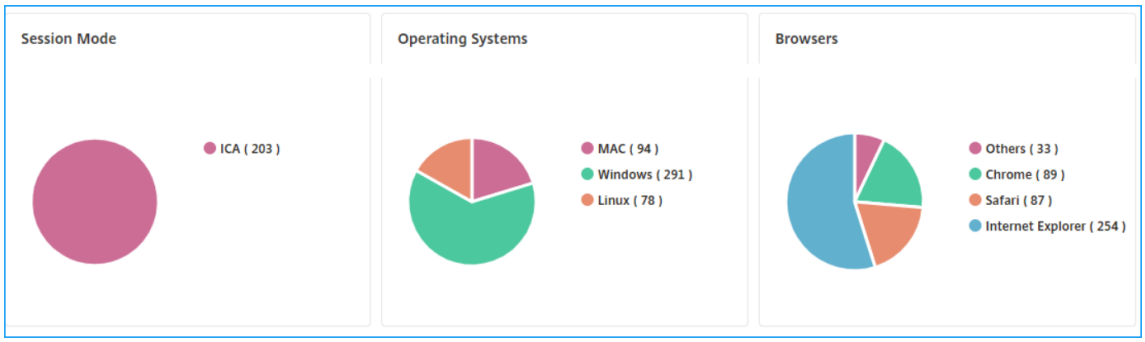
向下滚动可查看可用用户和活动用户列表。



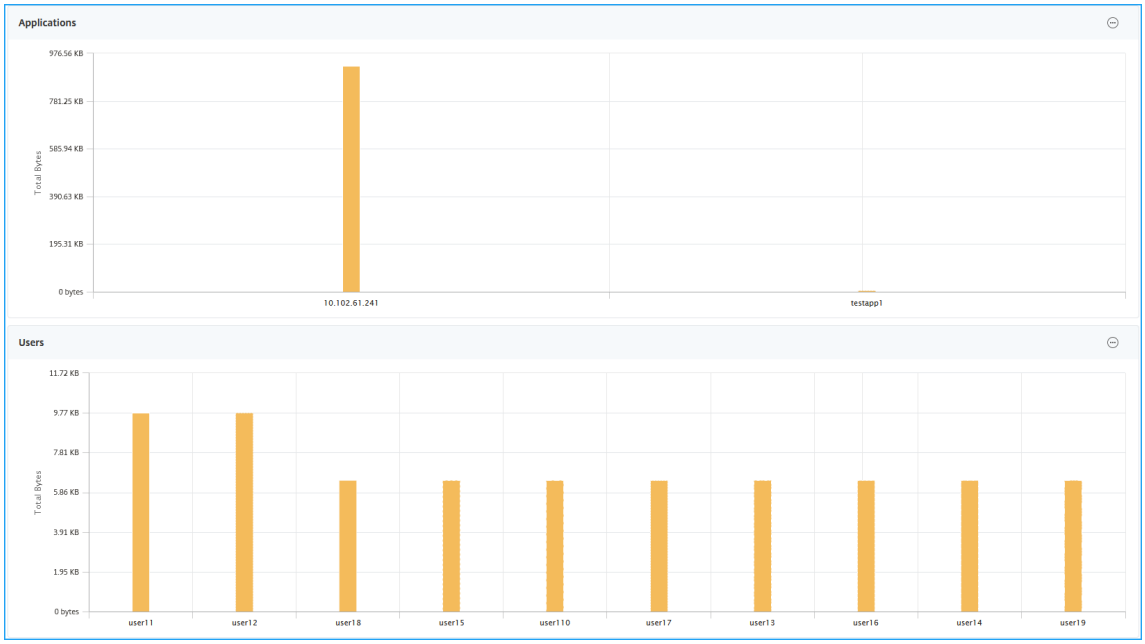
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

在“用户”或“活动用户”选项卡上，单击用户可查看以下用户详细信息：

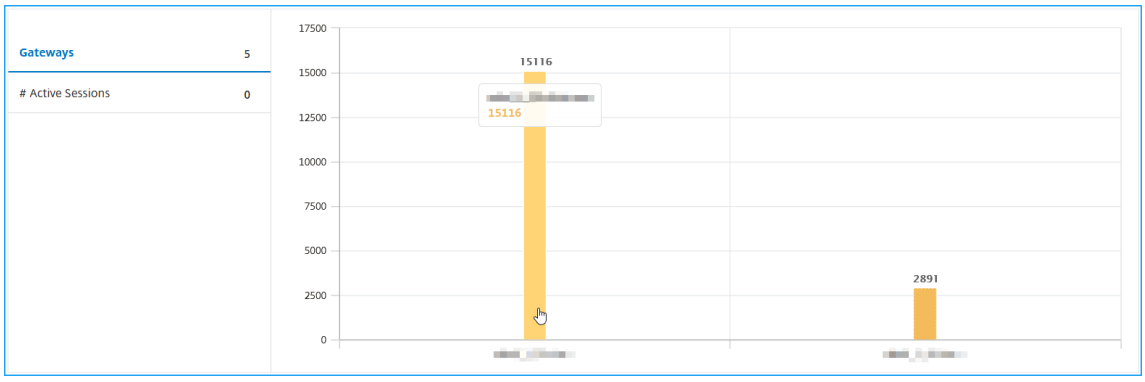
- 用户详情 -您可以查看与 NetScaler Gateway 设备关联的每位用户的见解。导航到网关 > **Gateway Insight** > 用户，然后单击用户以查看所选用户的见解，例如会话模式、操作系统和浏览器。



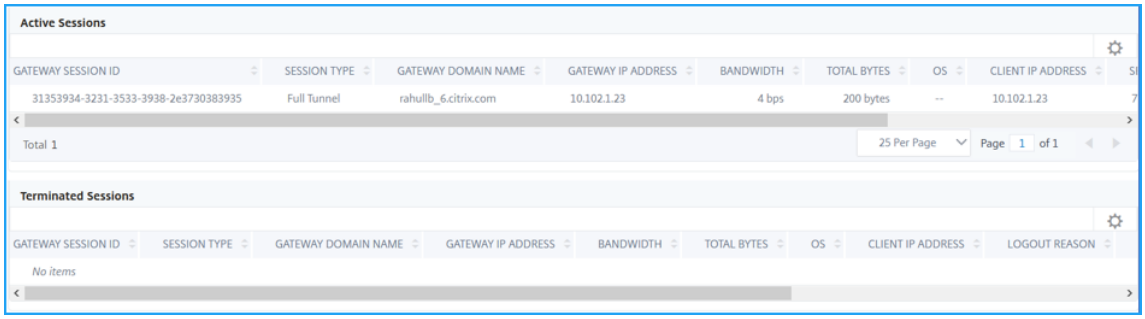
- 选定网关的用户和应用程序 - 导航到网关 > **Gateway Insight** > 网关，然后单击网关域名以查看与所选网关关联的前 10 个应用程序和前 10 个用户。



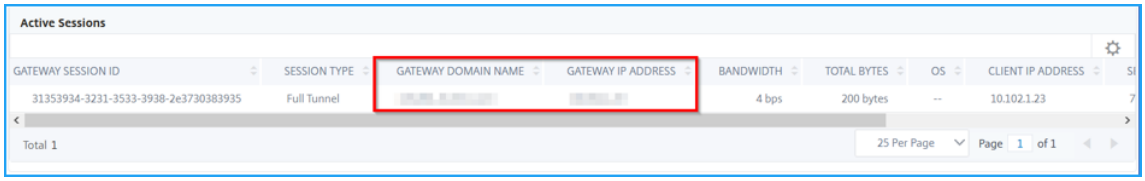
- 查看应用程序和用户的更多选项—对于 10 个以上的应用程序和用户，您可以单击应用程序和用户中的更多图标以查看与所选网关关联的所有用户和应用程序详细信息。
- 通过单击条形图查看详细信息—单击条形图时，可以查看相关详细信息。例如，导航到网关 **> Gateway Insight >** 网关，然后单击网关条形图以查看网关详细信息。



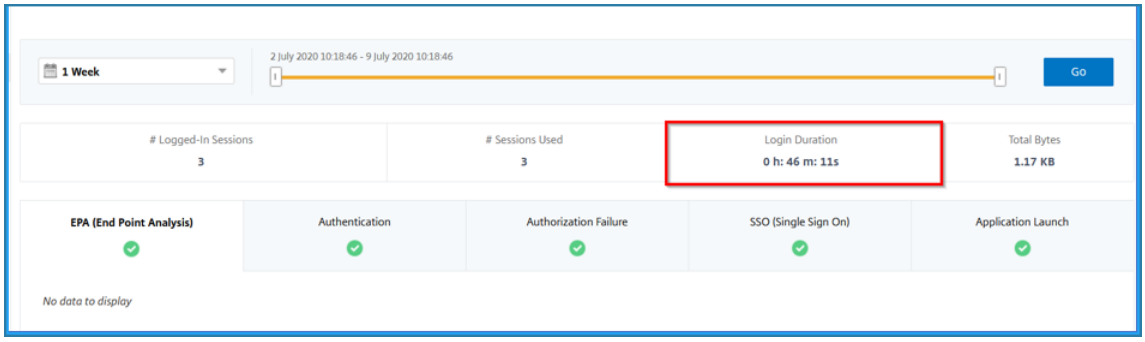
- 用户 活动会话 和 已终止的会话。



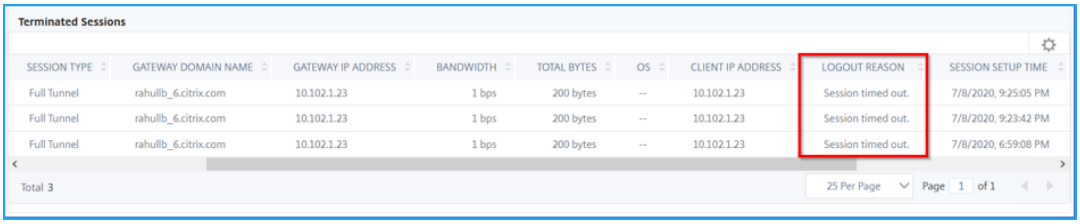
- 活动会话中的网关域名和网关 IP 地址。



- 用户登录持续时间。



- 用户注销会话的原因。注销的原因可能是：
  - 会话超时
  - 由于内部错误而注销
  - 由于非活动会话超时而注销
  - 用户已注销
  - 管理员已停止会话



搜索栏和 **Geo** 地图视图

您可以查看：

- 使您能够根据用户名筛选结果的搜索栏。导航到 网关 **> Gateway Insight >** 用户，查看 用户 和 活跃用户的搜索栏。将鼠标指针放在搜索栏上，选择 用户名，然后键入用户名以筛选结果。

- 基于用户地理位置显示用户信息的地理地图。作为管理员，使用此地理地图，您可以查看特定位置的用户总数、应用程序总数和会话总数的摘要。

  1. 导航到 网关 **> Gateway Insight** 查看地理地图
  2. 单击国家/地区。例如，美国

     地理地图显示所选国家/地区的用户列表、活动会话、已终止的会话、应用程序等详细信息。

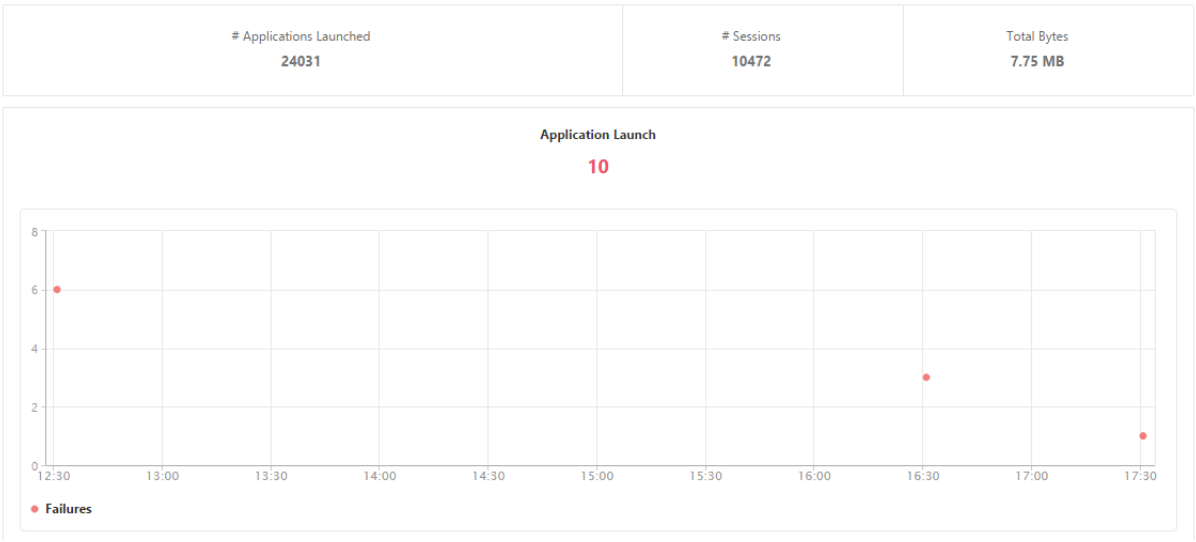
应用程序

可以查看启动的应用程序数、总会话数和活动会话数、应用程序使用的总字节数和带宽。可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

查看应用程序详细信息

1. 在 NetScaler 控制台中，导航 到 **Gateway > Gateway Insight >** 应用程序。
2. 选择要查看应用程序详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

现在可以查看启动的应用程序数、总会话数和活动会话数、应用程序使用的总字节数和带宽。



向下滚动可查看 ICA 和其他应用程序使用的会话数、带宽及总字节数。

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

在其他应用程序选项卡上，您可以单击名称列中的应用程序以显示该应用程序的详细信息。

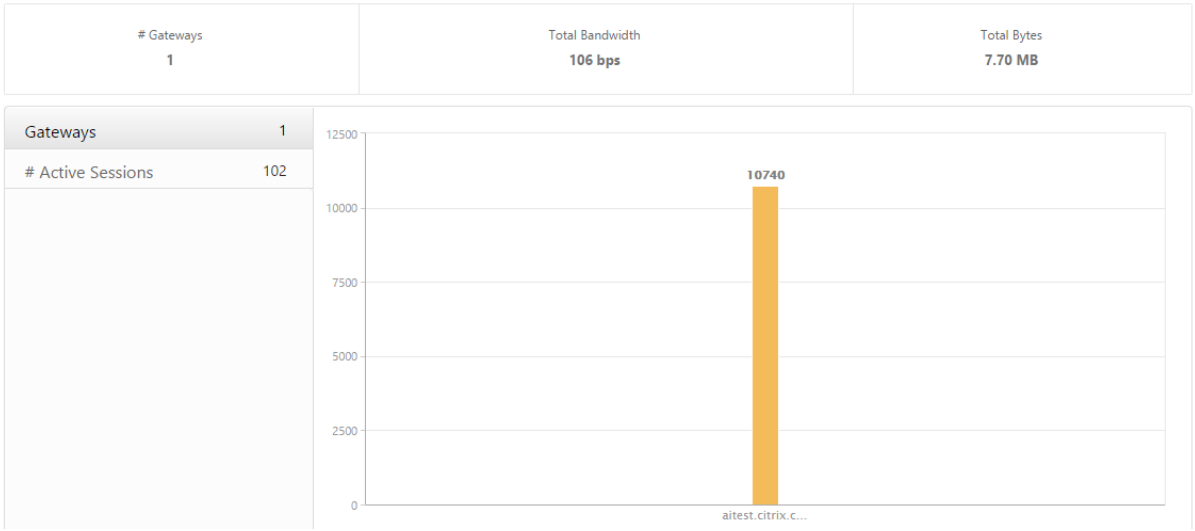
网关

您可以在任何给定时间查看与 NetScaler Gateway 设备关联的所有网关使用的网关数、活动会话数、总字节数和带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其登录活动的详细信息。

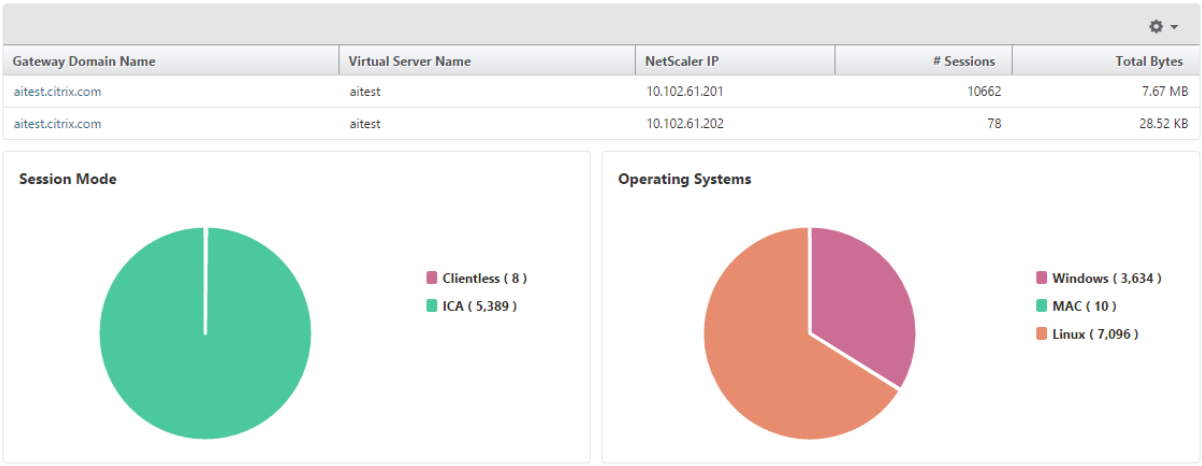
查看网关详情

1. 在 NetScaler 控制台中，导航到 **Gateway > Gateway Insight > Gateway Insight >** 网关。
2. 选择要查看网关详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

现在可以查看任何给定时间的网关数、活动会话数、与 NetScaler Gateway 设备关联的所有网关使用的总字节数和带宽。



向下滚动可查看网关详细信息，例如，“Gateway Domain Name”（网关域名）、“Virtual Server Name”（虚拟服务器名称）、NetScaler IP 地址、会话模式及“Total Bytes”（总字节数）。



您可以单击 Gateway 域名列中的 **Gateway** ，以显示网关的 EPA、身份验证、单点登录和应用程序启动失败以及其他详细信息。

您还可以查看网关的地理地图，使您能够根据特定位置筛选用户。

1. 导航到 网关 **> Gateway Insight >** 网关
2. 选择网关域名以查看地理地图
3. 单击国家/地区。例如，美国

   地理地图显示所选国家/地区的用户列表、活动会话、已终止的会话、应用程序等详细信息。

导出报告

您可以在本地计算机上以 PDF、JPEG、PNG 或 CSV 格式将 GUI 中显示的所有详细信息保存 Gateway Insight 报告。您还可以计划以各种时间间隔将报告导出到指定的电子邮件地址。

> 注意
>
> - 具有只读访问权限的用户不能导出报告。
> - 仅当 NetScaler 控制台具有互联网连接时，才会导出地理地图报告。

导出报告

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“立即导出”下，选择所需的格式，然后单击“导出”。

要计划导出：

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“计划导出”下，指定详细信息并单击“计划”。

要编辑导出时间表，请执行以下操作：

1. 在配置选项卡上，导航到 配置 > **NetScaler Insight Center** > 导出计划。
2. 从可用列表中选择一个报告，然后单击“编辑”。
3. 编辑后，单击“保存”。

> 注意
>
> 在计划报告之前，请导航到“系统”>“通知”>“电子邮件”，然后单击“添加”，配置 电子邮件服务器设置。

要添加电子邮件服务器或电子邮件通讯组列表，请执行以下操作：

1. 在“配置”选项卡上，导航到“系统”>“通知”>“电子邮件”。
2. 在右侧窗格中，选择“电子邮件服务器”以添加电子邮件服务器，或选择“电子邮件分发列表”以创建电子邮件通讯组列表。
3. 指定详细信息，然后单击“创建”。

要导出整个 **Gateway Insight** 控制板：

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“立即导出”下，选择 **PDF** 格式，然后单击“导出”。

Gateway Insight 用例

以下使用案例展示了如何使用 Gateway Insight 在 NetScaler Gateway 设备上查看用户的访问详细信息、应用程序和网关。

1. 用户无法登录到 NetScaler Gateway 设备或内部 Web 服务器

您是 NetScaler Gateway 管理员，通过 NetScaler 控制台监视 NetScaler Gateway 设备，您想了解用户无法登录的原因，或者故障发生在登录过程的哪个阶段。

NetScaler 控制台使您能够在登录过程的以下阶段查看用户登录错误的详细信息：

- 身份验证
- 端点分析 (EPA)
- 单点登录

在 NetScaler 控制台中，您可以搜索特定用户，然后查看该用户的所有详细信息。

要搜索用户，请执行以下操作：

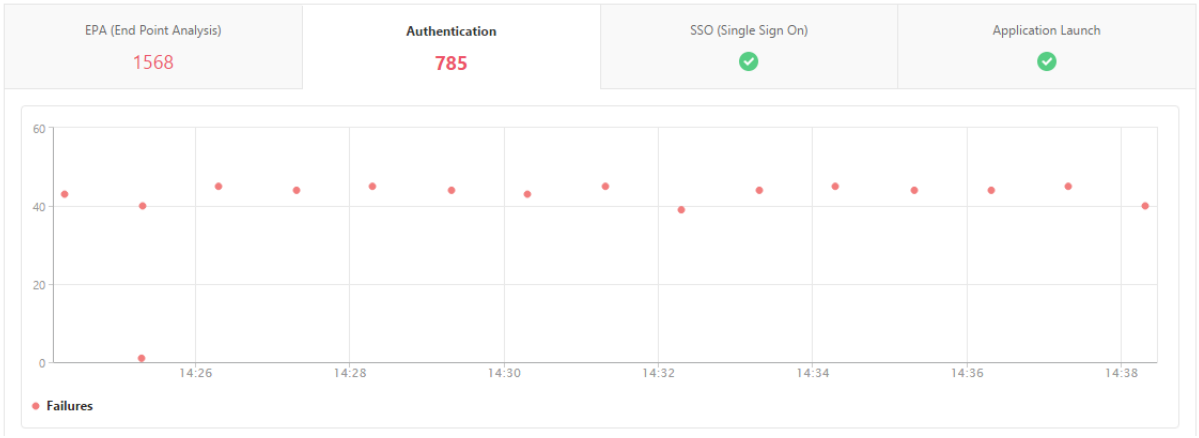
在 NetScaler 控制台中，导航 到 **Gateway > Gateway Insight**，然后在“搜索 用户”文本框中指定要搜索的用户。

身份验证失败

可以查看身份验证错误，例如，凭据错误或身份验证服务器没有响应。如果设置了两个阶段的身份验证，可以查看是身份验证的主阶段、次阶段还是两个阶段失败。

查看身份验证失败的详细信息

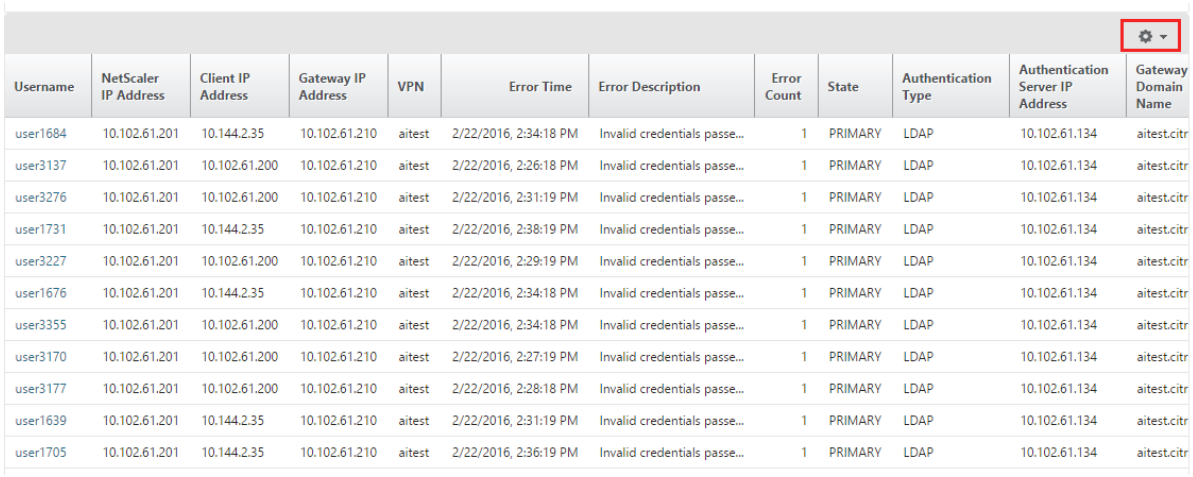
1. 在 NetScaler 控制台中，导航到 **Gateway >** GatewayInsight。
2. 在概述部分中，选择要查看身份验证错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 单击身份验证选项卡。您可以在故障图中查看任何给定时间的身份验证错误数量。



在同一选项卡上的表中向下滚动可查看每个身份验证错误的详细信息，例如，**Username**（用户名）、**Client IP Address**（客户端 **IP** 地址）、**Error Time**（错误时间）、**Authentication Type**（身份验证类型）、**Authentication Server IP Address**（身份验证服务器 **IP** 地址）及其他信息。表中的错误描述列显示登录失败的原因，状态列显示在两阶段身份验证的哪个阶段发生失败。

您可以单击“用户 名”列中的用户以显示该用户的身份验证错误和其他详细信息。

您可以使用设置选项自定义表格以添加或删除列。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

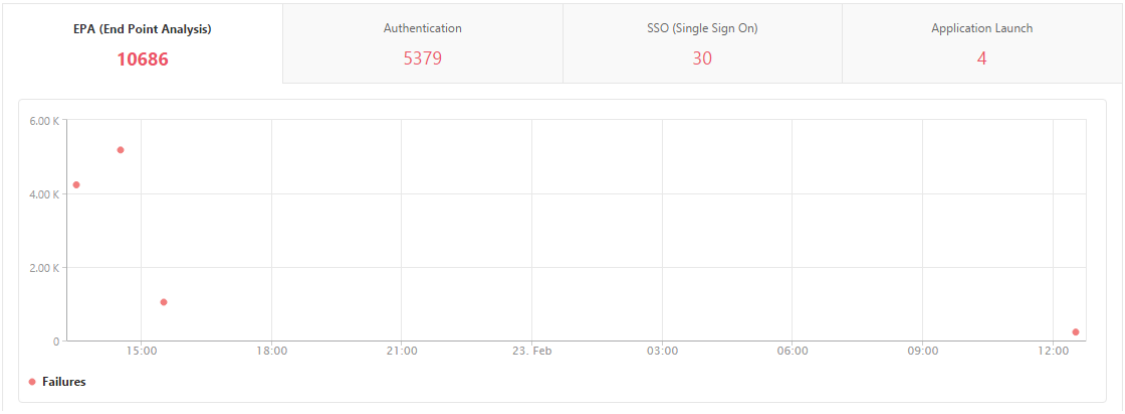
EPA 失败

您可以在身份验证前或身份验证后阶段查看 EPA 故障。

查看 **EPA** 失败详情

1. 在 NetScaler 控制台中，导航到 **Gateway >** GatewayInsight。
2. 在“Overview”（概述）部分中，选择要查看 EPA 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

3. 单击 **EPA**（终点分析）选项卡。您可以在故障图中查看任何给定时间的 EPA 错误数。



在同一选项卡上的表中向下滚动可查看每个 EPA 错误的详细信息，例如，**Username**（用户名）、**NetScaler IP Address**（**NetScaler IP** 地址）、**Gateway IP Address**（网关 **IP** 地址）、**VPN**、**Error Time**（错误时间）、**Policy Name**（策略名称）、**Gateway Domain Name**（网关域名）及其他信息。表中 **Error Description**（错误说明）列显示 EPA 失败的原因，**Policy Name**（策略名称）列显示导致失败的策略。

您可以单击“用户 名”列中的用户以显示该用户的 EPA 错误和其他详细信息。

您可以使用设置选项自定义表格以添加或删除列。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

> 注意
>
> 当将“ClientSecurity”表达式配置为 VPN 会话策略规则时，NetScaler Gateway 不会报告 EPA 故障。

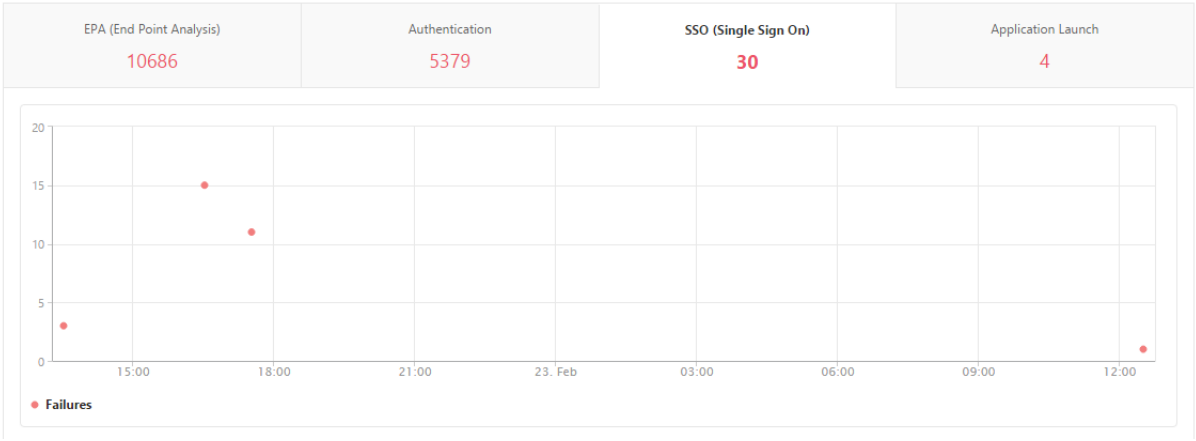
SSO 失败

可以查看通过 NetScaler Gateway 设备访问任何应用程序的用户在任何阶段的所有 SSO 失败。

查看 **SSO** 失败详情

1. 在 NetScaler 控制台中，导航到 **Gateway >** GatewayInsight。
2. 在“Overview”（概览）部分中，选择要查看 SSO 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

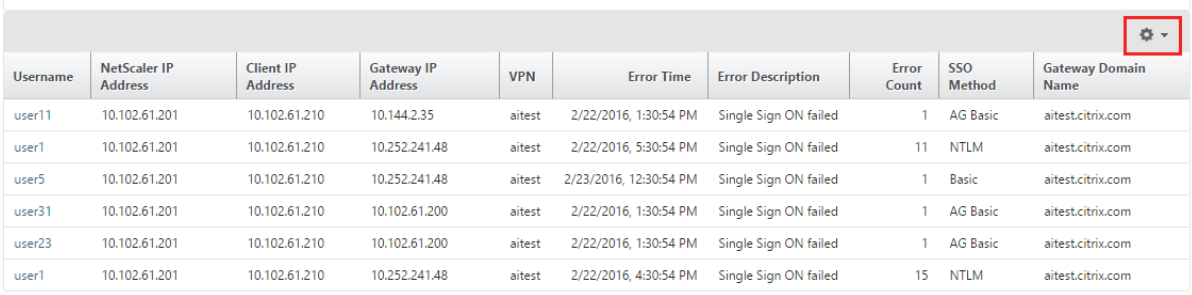
3. 单击 **SSO**（单次登录）选项卡。可以在“Failures”（失败）图中查看任何给定时间的 SSO 错误数。



在同一选项卡上的表中向下滚动可查看每个 SSO 错误的详细信息，例如，**Username**（用户名）、**NetScaler IP Address**（**NetScaler IP** 地址）、**Error Time**（错误时间）、**Error Description**（错误说明）、**Resource Name**（资源名称）及其他信息。

您可以单击“用户 名”列中的用户以显示该用户的 SSO 错误和其他详细信息。

您可以使用设置选项自定义表格以添加或删除列。

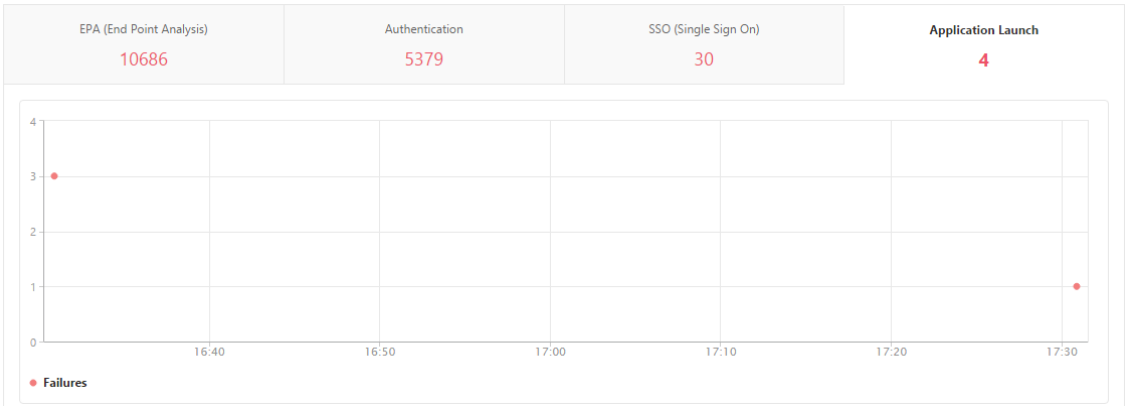


Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

2. 成功登录到 **NetScaler Gateway** 后，用户将无法启动任何虚拟应用程序　对于应用程序启动失败，您可以了解原因，例如无法访问的安全票证颁发机构 (STA) 或 Citrix 虚拟应用程序服务器或 STA 票证无效。可以查看错误发生的时间、错误的详细信息以及 STA 验证失败的资源。

查看应用程序启动失败的详细信息

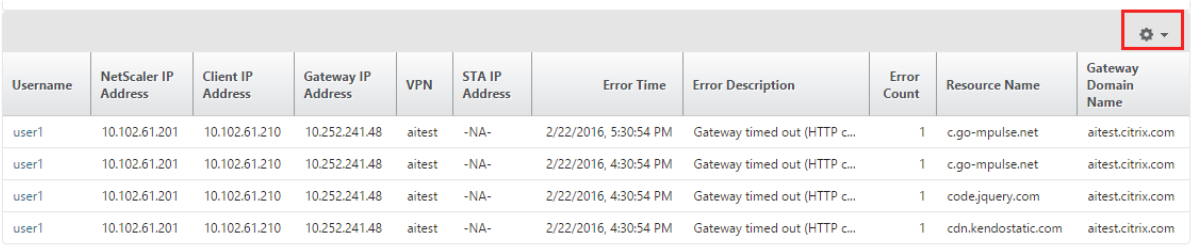
1. 在 NetScaler 控制台中，导航到 **Gateway >** GatewayInsight。
2. 在概述部分中，选择要查看 SSO 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 单击应用程序启动选项卡。您可以在失败图表中查看任何给定时间的应用程序启动失败次数。



在同一选项卡上的表中向下滚动可查看每个应用程序启动错误的详细信息，例如，**NetScaler IP Address**（**NetScaler IP** 地址）、**Error Time**（错误时间）、**Error Description**（错误说明）、**Resource Name**（资源名称）、**Gateway Domain Name**（网关域名）及其他信息。表中的 **Error Description**（错误说明）列显示 STA 服务器的 IP 地址，**Resource Name**（资源名称）列显示 STA 验证失败的资源的详细信息。

您可以单击“用户 名”列中的用户以显示该用户的应用程序启动错误和其他详细信息。

您可以使用设置选项自定义表格以添加或删除列。

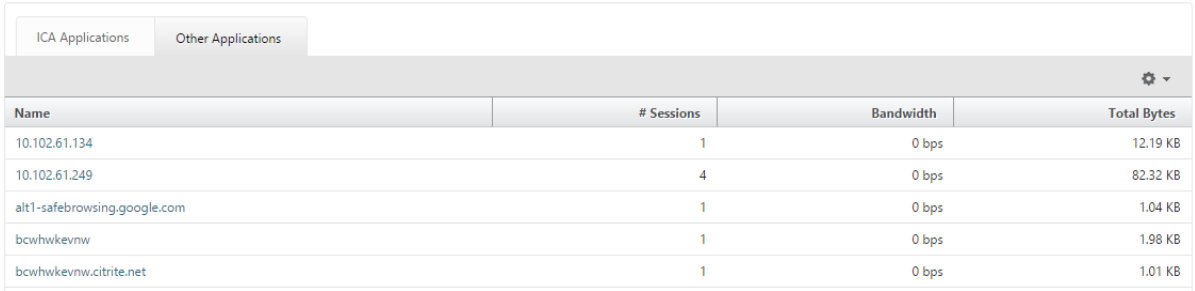


Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

3. 成功启动新应用程序后，用户希望查看该应用程序占用的总字节和带宽　成功启动新应用后，您可以在 NetScaler 控制台中查看该应用消耗的总字节数和带宽。

查看应用程序消耗的总字节数和带宽

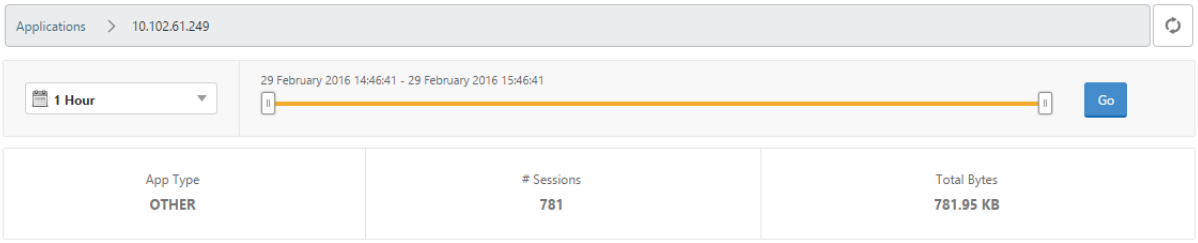
在 NetScaler 控制台中，导航 到 **Gateway > Gateway Insight** 应用程序，向下滚动，然后在“其他 应用程序”选项卡上，单击要查看详细信息的应用程序。



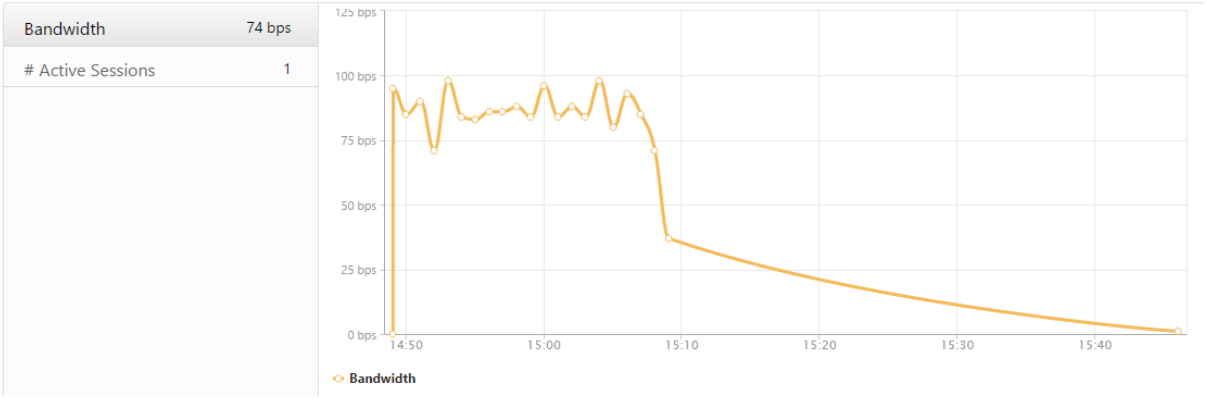
ICA Applications | Other Applications

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.134	1	0 bps	12.19 KB
10.102.61.249	4	0 bps	82.32 KB
alt1-safebrowsing.google.com	1	0 bps	1.04 KB
bcwhwkevnw	1	0 bps	1.98 KB
bcwhwkevnw.citrite.net	1	0 bps	1.01 KB

可以查看该应用程序使用的会话数和总字节数。



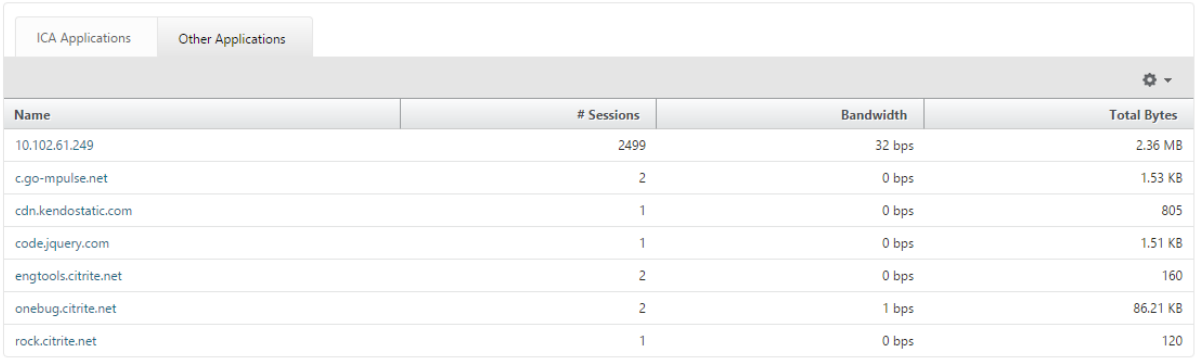
还可以查看该应用程序使用的带宽。



4. 用户已成功登录到 **NetScaler Gateway**，但无法访问内部网络中的某些网络资源　通过 Gateway Insight，可以确定用户是否有权访问网络资源。还可以查看导致失败的策略的名称。

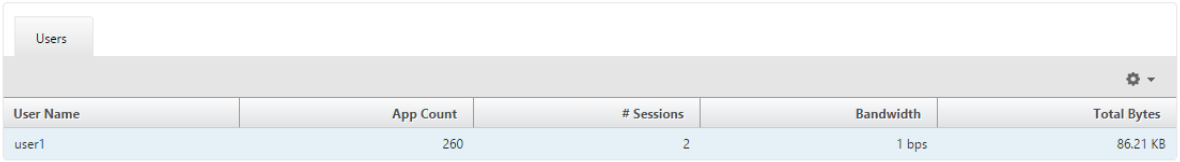
查看用户对资源的访问权限

1. 在 NetScaler 控制台中，导航 到 **Gateway > Gateway Insight >** 应用程序。
2. 在显示的屏幕上，向下滚动，在 **Other Applications**（其他应用程序）选项卡上，选择用户无法登录的应用程序。



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

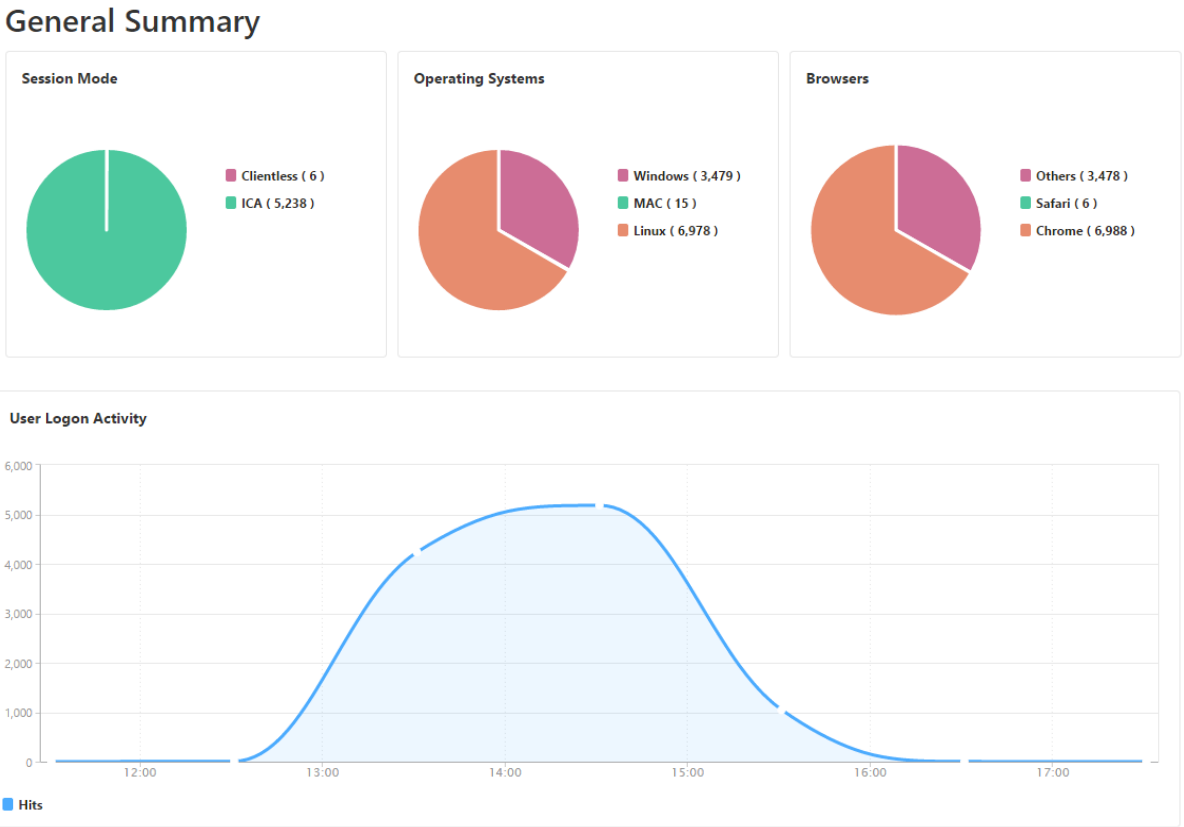
在出现的屏幕上向下滚动，并在“用户”表中显示有权访问该应用程序的所有用户。



5. 不同的用户可能正在使用不同的 **NetScaler Gateway** 部署，也可能通过不同的访问模式登录到 **NetScaler Gateway**。管理员必须能够查看有关部署类型和访问模式的详细信息　通过 Gateway Insight，可以查看用户用于登录的不同会话模式、客户端类型及每小时登录用户数的摘要。您还可以确定用户的部署是统一网关还是经典 NetScaler Gateway 部署。对于 Unified Gateway 部署，可以查看内容交换虚拟服务器名称和 IP 地址及 VPN 虚拟服务器名称。

查看会话模式、客户端类型和登录用户数的摘要

1. 在 NetScaler 控制台中，导航到 **Gateway >** GatewayInsight。
2. 在概述部分中，向下滚动以查看会话模式、操作系统、浏览器和用户登录活动图表显示用户用于登录的不同会话模式、客户端类型以及每小时登录的用户数。



HDX Insight

January 29, 2024

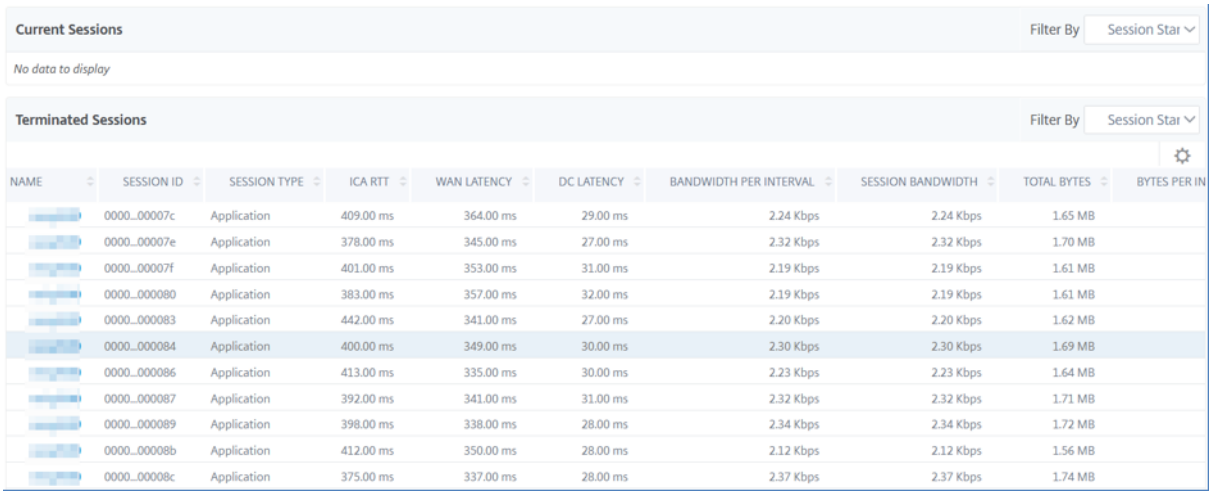
HDX Insight 为通过 NetScaler 流向 Citrix Virtual Apps and Desktops 的 HDX 流量提供端到端可见性。它还让管理员能够查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。实时和历史可见性数据的可用性使 NetScaler 控制台能够支持各种用例。

要显示任何数据，您需要在 NetScaler Gateway 虚拟服务器上启用 AppFlow。AppFlow 可以通过 **IPFIX** 协议或 **Logstream** 方法交付。

> 注意
>
> 要允许记录 ICA 往返时间计算，请启用以下策略设置：
>
> - ICA 往返行程计算
> - ICA 往返行程计算间隔
> - 空闲连接的 ICA 往返行程计算

如果单击单个用户，则可以看到该用户在所选时间范围内创建的每个 HDX 会话，无论是活动的还是终止的。其他信息包括会话期间消耗的几个延迟统计信息和带宽。您还可以从单个虚拟通道（如音频、打印机映射和客户端驱动器映射）获取带宽信息。

您还可以直观显示所有用户活动和已终止会话的合并视图。



作为管理员，此视图使您能够：

- 在单窗格可视化中查看所有用户详细信息
- 消除选择每个用户以及查看活动和已终止会话的复杂性

> 注意
>
> 创建组时，您可以为组分配角色、提供对组的应用程序级别访问权限以及将用户分配给组。NetScaler 控制台分析现在支持基于虚拟 IP 地址的授权。您的用户现在只能看到他们被授权的应用程序（虚拟服务器）的所有见解报告。有关组和向组分配用户的详细信息，请参见 在 NetScaler 控制台上配置组。

您也可以导航到 **HDX Insight** > 应用程序，然后单击“启动持续时间”以查看应用程序启动所花费的时间。您还可以通过导航到 **HDX Insight >** 用户来查看所有已连接用户的用户代理。

> 注意
>
> HDX Insight 支持在软件版本 12.0 上运行的 NetScaler 实例中配置管理分区。

下列瘦客户端支持 HDX Insight:

- WYSE 基于 Windows 的瘦客户端
- WYSE 基于 Linux 的瘦客户端
- WYSE 基于 ThinOS 的瘦客户端
- 基于 10ZiG Ubuntu 的瘦客户端

找出低性能问题的根本原因

场景 **1**

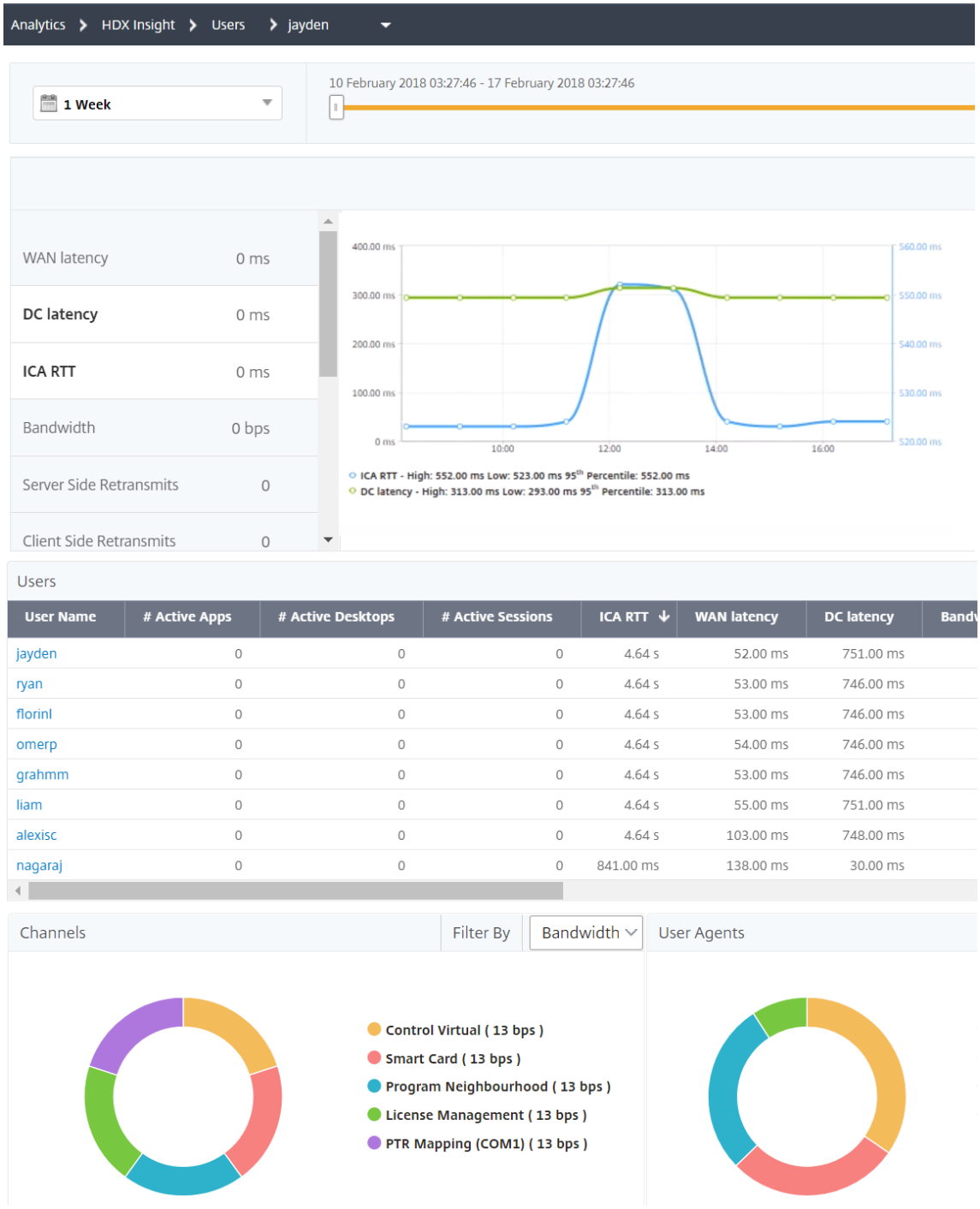
用户在访问 **Citrix Virtual Apps and Desktops** 时遇到延迟　延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟或客户端网络延迟造成。

为了找出问题的根本原因，请分析下列指标:

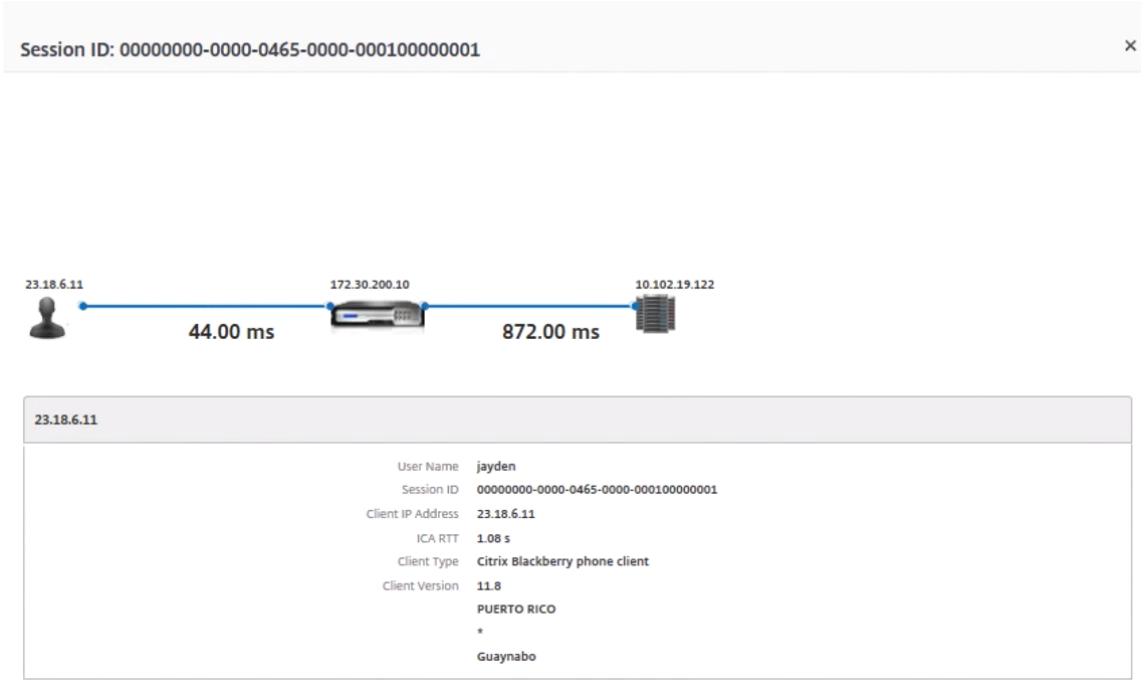
- WAN 延迟
- DC 延迟
- 主机延迟

要查看客户端度量，请执行以下操作:

1. 在分析选项卡上，导航到 **HDX Insight** > 用户。
2. 向下滚动并选择用户名，然后从列表中选择句点。期间可以是一天、一周、一个月，甚至可以自定义要查看数据的期间。
3. 图表以图形形式显示用户在指定时间段内的 ICA RTT 和 DC 延迟值。



4. 在当前应用程序会话表中，将鼠标悬停在 **RTT** 值上，并记下主机延迟、DC 延迟和 WAN 延迟值。
5. 在当前应用程序会话表中，单击跳图符号以显示有关客户端和服务器之间连接的信息，包括延迟值。



摘要：

在此示例中，**DC** 延迟为 751 毫秒，**WAN** 延迟为 52 毫秒，主机延迟为 6 秒。这表示由于服务器网络导致的平均延迟，用户正在遇到延迟。

方案 **2**

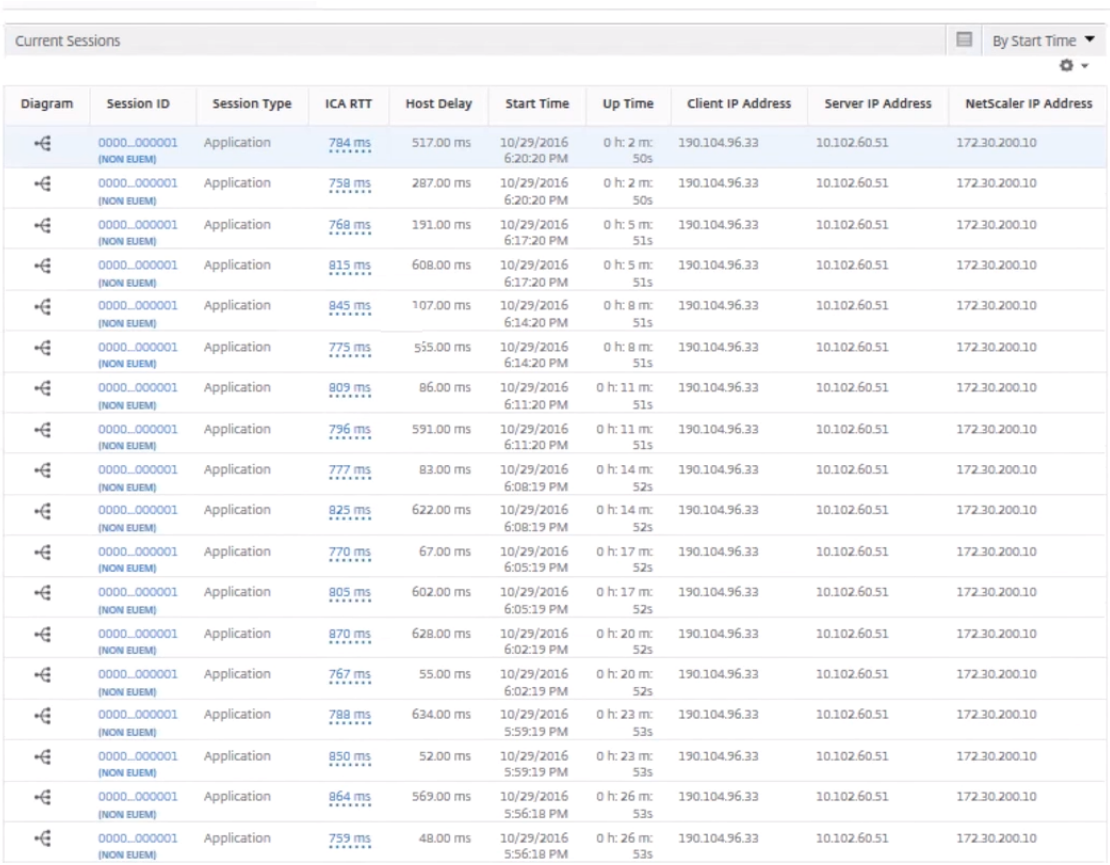
用户在 **Citrix Virtual Apps** 或 **Citrix Virtual Desktops** 上启动应用程序时遇到延迟　延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟、客户端网络延迟或应用程序启动所用时间造成。

为了找出问题的根本原因，请分析下列指标：

- WAN 延迟
- DC 延迟
- 主机延迟

要查看用户指标，请执行以下操作：

1. 导航到网关 > **HDX Insight** > 用户。
2. 向下滚动并单击用户名。
3. 在图形表示方式中，注意观察特定会话的 WAN 延迟、DC 延迟以及 RTT 值。
4. 在当前应用程序会话表中，请注意，主机延迟很高。



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

摘要：

在此示例中，**DC** 延迟为 1 毫秒，**WAN** 延迟为 12 毫秒，但主机延迟为 517 毫秒。高 RTT 且直流和 WAN 延迟较低，表示主机服务器上出现应用程序错误。

> 注
>
> 意：如果您使用运行软件 11.1 版本 51.21 或更高版本的 NetScaler 控制台，HDX Insight 还会显示更多用户指标，例如广域网抖动和服务器端重传。要查看这些指标，请导航到网关 > **HDX Insight** > 用户，然后选择一个用户名。用户指标将显示在图旁边的表中。

HDX Insight 的地理地图

NetScaler 控制台中的地理地图功能在地图上显示了不同地理位置的 Web 应用程序的使用情况。作为管理员，您可以使用此信息了解应用程序使用趋势和容量规划。

Geo map 提供了有关特定于国家/地区、州和城市的以下指标的信息：

- 点击总数：访问应用程序的总次数。
- 带宽：服务客户端请求时消耗的总带宽
- 响应时间：向客户端请求发送响应所用的平均时间。

Geo map 提供的信息可用于解决以下几种用例：

- 访问应用程序的客户端数最大的区域
- 响应时间最长的区域
- 消耗最多带宽的区域

当您启用 **Web** 洞察时，NetScaler 控制台会自动 启用私有 IP 地址或公有 IP 地址的地理地图。

创建私有 IP 块

当客户端私有 IP 地址添加到 NetScaler 控制台服务器时，NetScaler 控制台可以识别客户端的位置。例如，如果客户端的 IP 地址在与城市 A 相关的私有 IP 地址块范围内，则 NetScaler 控制台会识别出该客户端的流量来自城市 A。

要创建 IP 块，请执行以下操作：

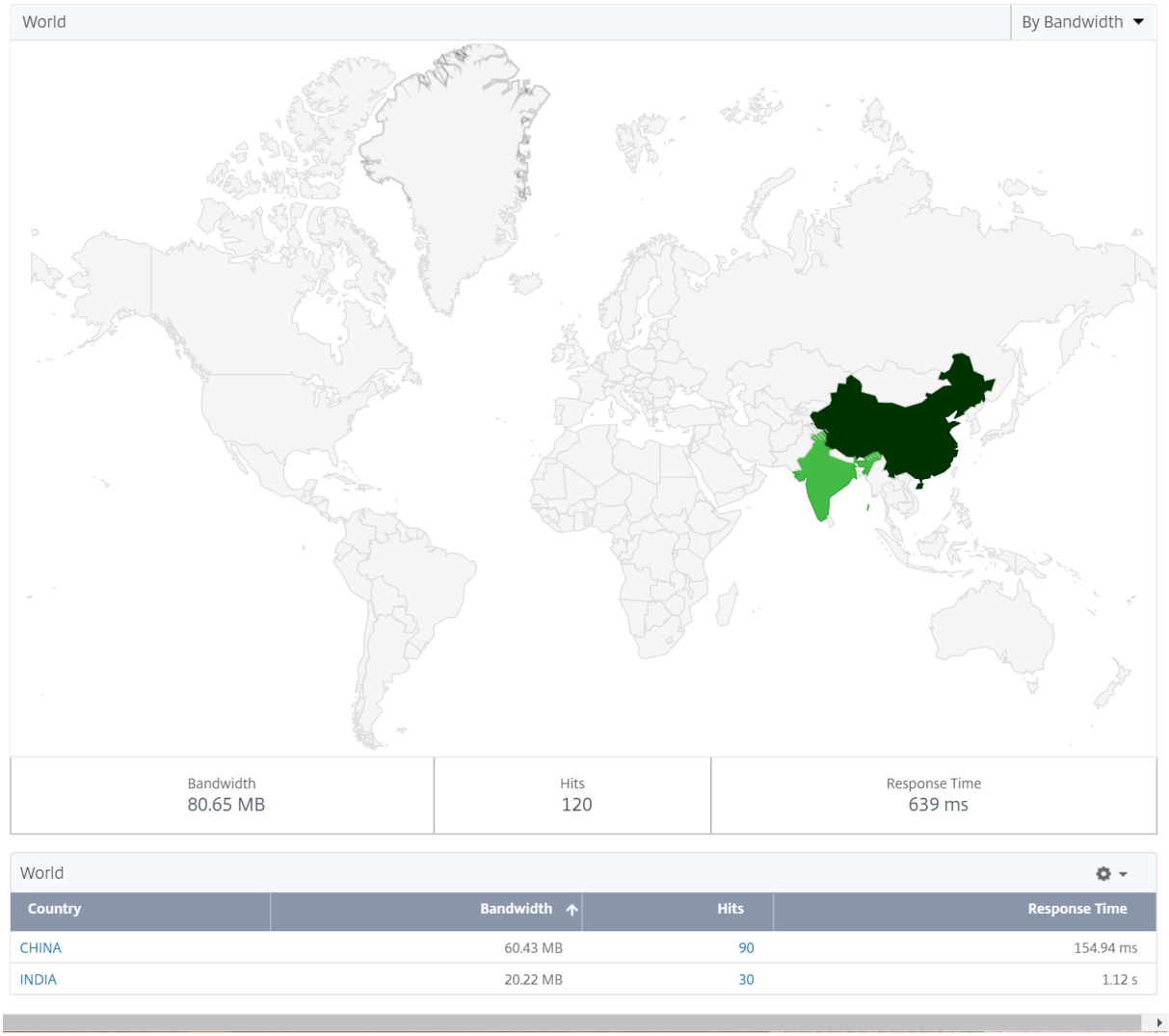
1. 在 NetScaler 控制台中，导航到“设置”**>**“分析设置”**>**“**IP** 块”，然后单击“添加”。
2. 在创建 **IP** 块页面中，指定以下参数：

- 名称。为私有 IP 块指定一个名称
- 起始 **IP** 地址。指定 IP 块的最低 IP 地址范围。
- 结束 **IP** 地址。指定 IP 块的最大 IP 地址范围。
- 国家。从列表中选择国家。
- 区域。根据国家/地区，该区域会自动填充，但您可以选择您的区域。
- 城市。根据地区，城市会自动填充，但您可以选择您的城市。
- 城市纬度和城市经度。根据您选择的城市，纬度和经度会自动填充。

3. 单击 **Create**（创建）完成。

公共 **IP** 块　如果客户端使用公有 IP 地址，NetScaler 控制台还可以识别客户端的位置。NetScaler 控制台有其内置位置 CSV 文件，该文件根据客户端 IP 地址范围匹配位置。要使用公共 IP 区块，唯一的要求是您必须从“配置洞察”页面启用“启用地理数据收集”。

> 注意
>
> NetScaler 控制台需要互联网连接才能显示特定地理位置的地理地图。还需要 Internet 连接才能以.pdf、.png 或.jpg 格式导出 GeoMap。



要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每天、每周或每月发送报告，并通过电子邮件或 Slack 消息发送报告。

> 注意
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

要为数据中心配置地理图，请执行以下操作：

在“基础结构”选项卡上，导航到“站点”>“私有 **IP** 块”，为特定位置配置地理地图。

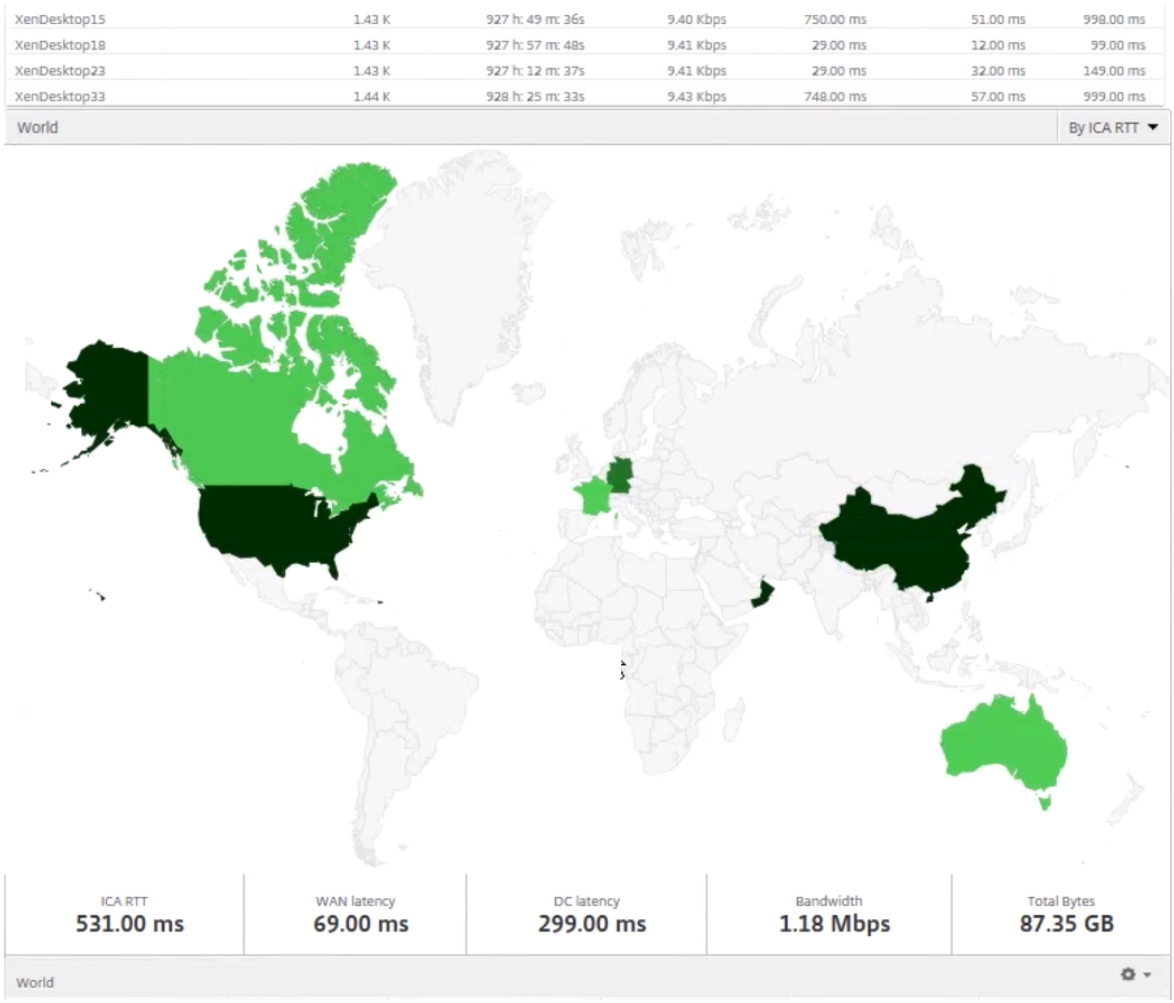
用例

假设这样一个场景：组织 ABC 有 2 个分支机构：一个在圣克拉拉，另一个在印度。

圣克拉拉的用户使用 NetScaler Gateway 设备连接到 SClara.x.com 来访问 VPN 流量。印度的用户使用 NetScaler Gateway 设备连接到 India.x.com 来访问 VPN 流量。

在一个特殊的时间间隔（例如 10 AM 到 5 PM），圣克拉拉的用户连接到 SClara.x.com 来访问 VPN 流量。大多数用户访问相同的 NetScaler Gateway，从而导致连接到 VPN 的延迟，因此某些用户连接到 India.x.com 而不是 SClara.x.com。

分析流量的 NetScaler 管理员可以使用地理地图功能来显示圣克拉拉办公室的流量。该地图显示圣克拉拉办公室的响应时间很长，因为圣克拉拉办公室只有一个 NetScaler Gateway 设备，用户可以通过该设备访问 VPN 流量。因此，管理员可能会决定安装另一个 NetScaler Gateway，以便用户有两个本地 NetScaler Gateway 设备来访问 VPN。



限制

如果 NetScaler 实例具有高级许可，则不会触发在 NetScaler 控制台上为 HDX Insight 设置的阈值，因为分析数据仅收集 1 小时。

要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每天、每周或每月发送报告，并通过电子邮件或 Slack 消息发送报告。

> 注意
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

启用 **HDX Insight** 数据收集

January 29, 2024

HDX Insight 通过提供通过 NetScaler 设备的 ICA 流量的端到端可见性，使管理员能够提供卓越的用户体验。

HDX Insight 为网络、虚拟桌面、应用程序和应用程序结构提供引人注目且强大的商业智能和故障分析功能。HDX Insight 可以即时鉴别分类用户问题、收集有关虚拟桌面连接的数据、生成 AppFlow 记录并将其呈现为可视报告。

在 NetScaler 实例中启用数据收集的配置因设备在部署拓扑中的位置而异。本主题包括以下详细信息：

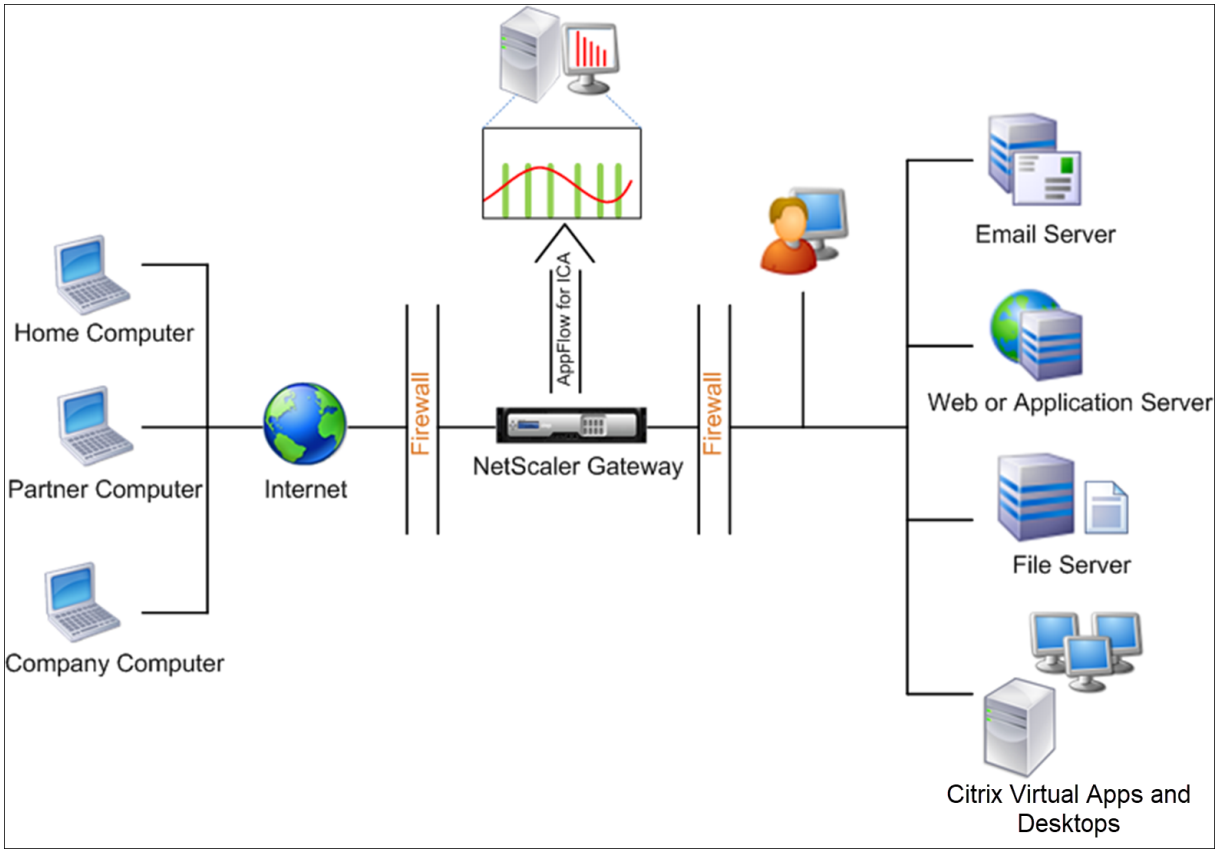
- 启用数据收集以监视以透明模式部署的 NetScaler 实例
- 为在单跃点模式下部署的 NetScaler Gateway 设备启用数据收集
- 为在双跃点模式下部署的 NetScaler Gateway 设备启用数据收集
- 启用数据收集以监视在局域网用户模式下部署的 NetScaler

为在单跃点模式下部署的 **NetScaler Gateway** 设备启用数据收集

January 29, 2024

NetScaler Gateway 以单跃点模式部署时，NetScaler Gateway 位于网络的边缘，并充当与桌面交付基础结构的 ICA 连接的代理。此部署是最简单、最常见的部署。此模式在外部用户尝试访问组织中的内部网络时提供安全性。在单跃点模式下，用户通过虚拟专用网络 (VPN) 访问 NetScaler 设备。

要开始收集报告，必须将 NetScaler Gateway 设备添加到 NetScaler 控制台清单中，并在 NetScaler 控制台上启用 AppFlow。下图说明了以单跳模式部署的 NetScaler 控制台



从 **NetScaler** 控制台启用 **AppFlow** 功能

1. 导航到 基础架构 > 实例，然后选择要启用分析的 NetScaler 实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。
3. 选择 VPN 虚拟服务器，然后单击“启用分析”。
4. 选择 **Web Insight**。
5. 单击确定。

> 注意
>
> ：在单跳模式下启用 AppFlow 时，以下命令开始在后台运行。此处显式指定这些命令是为了进行故障排除。
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`
> - `set appflow param -flowRecordInterval \<secs\>`
> - `disable ns feature AppFlow`

- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

启用数据收集以监视在透明模式下部署的 NetScaler

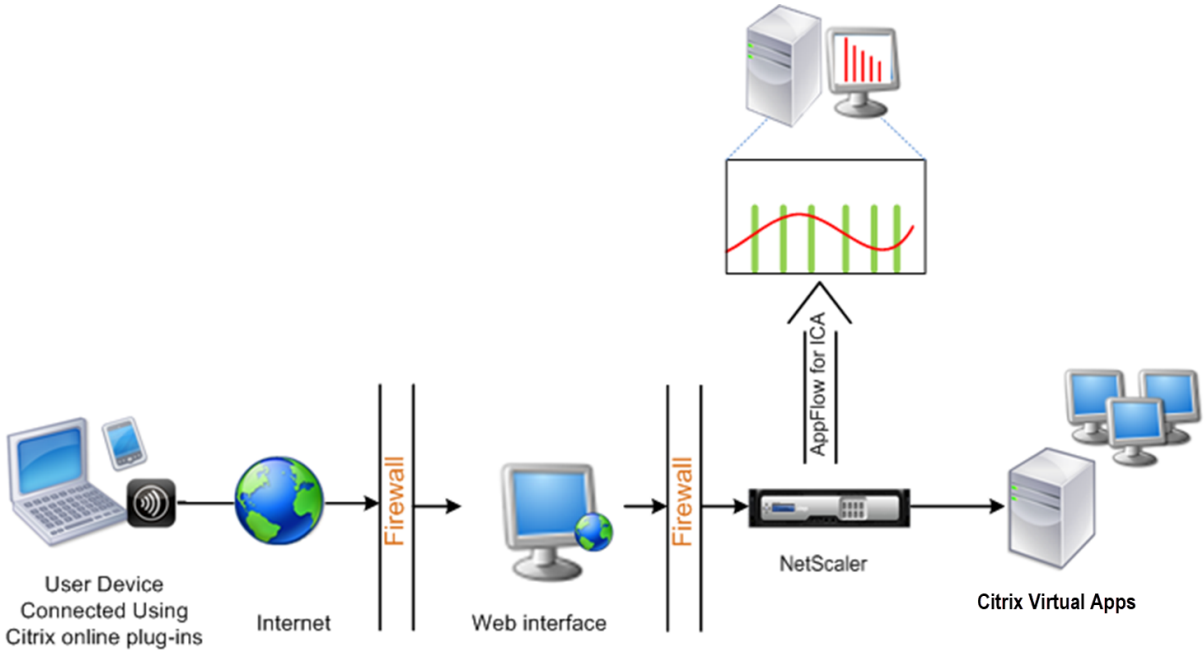
January 29, 2024

当以透明模式部署 NetScaler 时，客户端可以直接访问服务器，而无需干预虚拟服务器。如果 NetScaler 设备在 Citrix Virtual Apps and Desktops 环境中以透明模式部署，则 ICA 流量不会通过 VPN 传输。

将 NetScaler 添加到 NetScaler 控制台清单后，必须启用 AppFlow 进行数据收集。启用数据收集依赖于设备和模式。在这种情况下，您必须将 NetScaler 控制台添加为每台 NetScaler 设备上的 AppFlow 收集器，并且必须配置 AppFlow 策略以收集流经该设备的所有或特定 ICA 流量。

> 注意
>
> - 您无法使用 NetScaler 控制台配置实用程序在以透明模式部署的 NetScaler 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅命令参考。
> - 有关策略表达式的信息，请参阅策略和表达式。

下图显示了以透明模式部署 NetScaler 时 NetScaler 控制台的网络部署：



要使用命令行界面在 **NetScaler** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 指定 NetScaler 设备侦听流量所用的 ICA 端口。

```
set ns param --icaPorts \<port\>...
```

示例：

```
set ns param -icaPorts 2598 1494
```

> 注意
>
> - 可以使用此命令最多指定 10 个端口。
> - 默认端口号为 2598。可以根据需要修改端口号。

3. 将 NetScaler Insight Center 添加为 NetScaler 设备上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```


> 注意：
>
> 要查看 NetScaler 设备上配置的 AppFlow 收集器，请使用 **show appflow** 收集器 命令。

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action <name> -collectors <string> ...
```

示例：

```
add appflow action act -collectors MyInsight
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
```

示例：

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> 注意
>
> **type** 的值必须为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
```

8. 保存配置。

```
save ns config
```

为部署在双跃点模式下的 **NetScaler Gateway** 设备启用数据收集

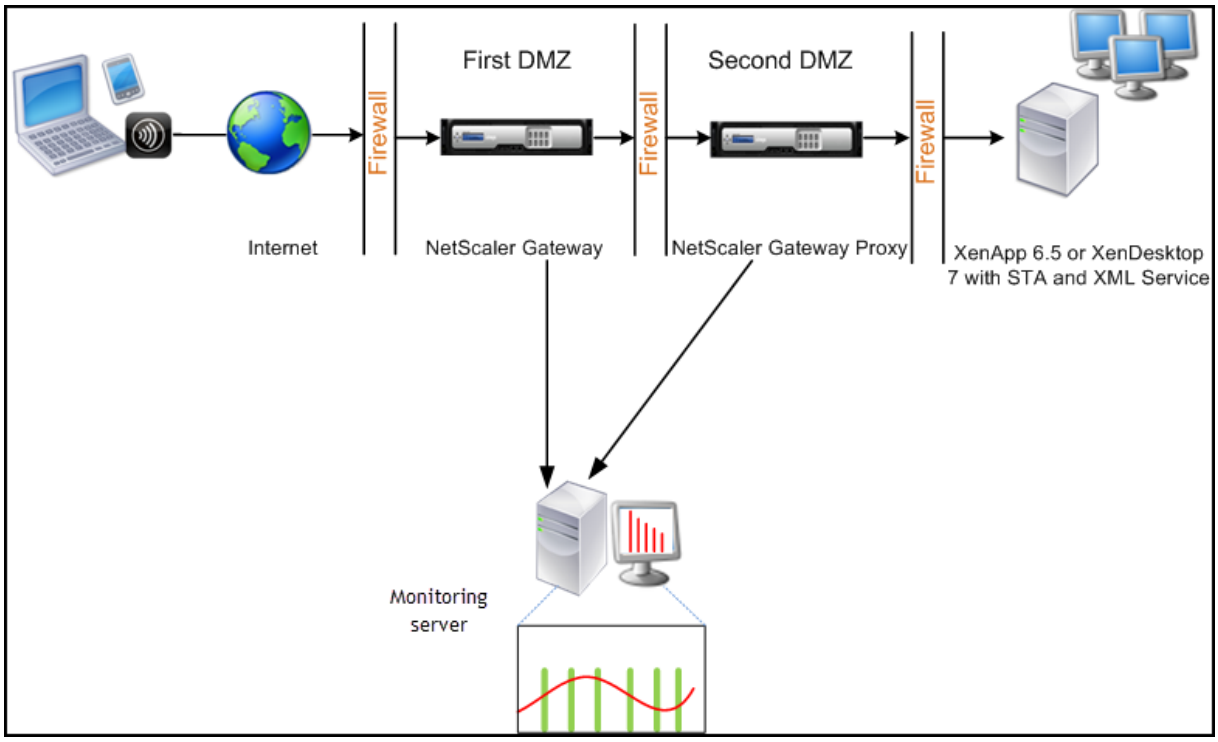
March 10, 2024

NetScaler Gateway 双跳模式为组织内部网络提供额外的保护，因为攻击者需要穿透多个安全区域或非军事区 (DMZ) 才能访问安全网络中的服务器。

作为管理员，您可以使用 NetScaler 控制台分析：

- ICA 连接通过的跳数（NetScaler Gateway 设备）
- 每个 TCP 连接的延迟以及它如何与客户端感知的总 ICA 延迟相关的详细信息

下图表明第一个 DMZ 中的 NetScaler 控制台和 NetScaler Gateway 部署在同一个子网中。



第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 NetScaler Gateway 充当 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够遍历第二个 DMZ，从而完成用户与服务器场的连接。

NetScaler 控制台可以部署在属于第一个 DMZ 中 NetScaler Gateway 设备的子网中，也可以部署在属于第二个 DMZ 的 NetScaler Gateway 设备的子网中。

在双跳模式下，NetScaler 控制台从一台设备收集 TCP 记录，从另一台设备收集 ICA 记录。将 NetScaler Gateway 设备添加到 NetScaler 控制台清单并启用数据收集后，每台设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 NetScaler 控制台识别哪个设备正在导出记录，每个设备都指定了跳数，每个连接都使用连接链 ID 指定。跃点数表示流量从客户端流向服务器的 NetScaler Gateway 设备的数量。连接链 ID 表示客户端与服务器之间的端到端连接。

NetScaler 控制台使用跳数和连接链 ID 来关联来自两个 NetScaler Gateway 设备的数据并生成报告。

要监视以此模式部署的 NetScaler Gateway 设备，必须先将 NetScaler Gateway 添加到 NetScaler 控制台清单，在 NetScaler 控制台上启用 AppFlow，然后在 NetScaler 控制台控制面板上查看报告。

在 **NetScaler** 控制台上启用数据收集

如果您启用 NetScaler 控制台开始从两个设备收集 ICA 详细信息，则收集的详细信息是多余的。要克服这种情况，您必须在第一台 NetScaler Gateway 设备上启用 AppFlow for TCP，然后在第二台设备上启用 AppFlow for ICA。通过这样做，其中一个装置导出 ICA AppFlow 记录，另一个装置则导出 TCP AppFlow 记录。这还节省解析 ICA 通信的处理时间。

要从 **NetScaler** 控制台启用 **AppFlow** 功能，请执行以下操作：

1. 导航到基础架构 > 实例，然后选择要启用分析的 NetScaler 实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。
3. 选择虚拟服务器，然后单击“启用安全和分析”。
4. 选择 **Web Insight**
5. 单击确定。

配置 **NetScaler Gateway** 设备以导出数据

安装 NetScaler Gateway 设备后，必须在 NetScaler Gateway 设备上配置以下设置，才能将报告导出到 NetScaler 控制台：

- 在第一个和第二个 DMZ 中配置 NetScaler Gateway 设备的虚拟服务器以相互通信。
- 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。
- 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。
- 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。
- 允许其中一个 NetScaler Gateway 设备导出 ICA 记录
- 允许其他 NetScaler Gateway 设备导出 TCP 记录：
- 在两个 NetScaler Gateway 设备上启用连接链接。

使用命令行界面配置 **NetScaler Gateway**：

1. 将第一个 DMZ 中的 NetScaler Gateway 虚拟服务器配置为与第二个 DMZ 中的 NetScaler Gateway 虚拟服务器进行通信。

---

add vpn nextHopServer [**-secure** (ON OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
```


2. 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。在第一个 DMZ 中的 NetScaler Gateway 上运行以下命令：

   bind vpn vserver <name> **-nextHopServer** <name>

   ```
   1 bind vpn vserver vs1 -nextHopServer nh1
   ```

3. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点和 AppFlow。

set vpn vserver [**-doubleHop** (ENABLED DISABLED)] [**- appflowLog** (ENABLED DISABLED)]

```
1 set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
```

4. 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。

set vpn vserver [**-authentication** (ON OFF)]

```
1 set vpn vserver vs -authentication OFF
```

5. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

   ```
   1 bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type
       OTHERTCP_REQUEST
   ```

6. 启用其他 NetScaler Gateway 设备以导出 ICA 记录：

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

   ```
   1 bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
       ICA_REQUEST
   ```

7. 在两个 NetScaler Gateway 设备上启用连接链接：

set appFlow param [**-connectionChaining** (ENABLED DISABLED)]

```
1 set appflow param -connectionChaining ENABLED
```

使用配置实用程序配置 **NetScaler Gateway**：

1. 将第一个 DMZ 中的 NetScaler Gateway 配置为与第二个 DMZ 中的 NetScaler Gateway 进行通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。

a) 在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在“高级”组中展开“已发布的应用程序”。

c) 单击 下一跳服务器，然后将下一跳服务器绑定到第二台 NetScaler Gateway 设备。

2. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。

a) 在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，然后在基本设置组中单击“编辑”图标。

c) 展开“更多”，选择“双跃点”，然后单击“确定”。

3. 在第二个 DMZ 中的 NetScaler Gateway 上禁用虚拟服务器上的身份验证。

a) 在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，然后在基本设置组中单击“编辑”图标。

c) 展开 更多，然后清除“启用身份验证”。

4. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。

a) 在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 + 图标，然后从 选择策略 列表中选择 **AppFlow** ，然后从 选择类型 列表中选择 其他 **TCP** 请求。

d) 单击继续。

e) 添加策略绑定，然后单击“关闭”。

5. 启用其他 NetScaler Gateway 设备以导出 ICA 记录：

a) 在“配置”选项卡上，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 + 图标，然后从 选择策略 列表中选择 **AppFlow** ，然后从 选择类型 列表中选择 其他 **TCP** 请求。

d) 单击继续。

e) 添加策略绑定，然后单击“关闭”。

6. 在两个 NetScaler Gateway 设备上启用连接链接。

a) 在配置选项卡上，导航到系统 > 应用流程。

b) 在右侧窗格的“设置”组中，单击“更改 **Appflow** 设置”。

c) 选择“连接链接”，然后单击“** 确定”。

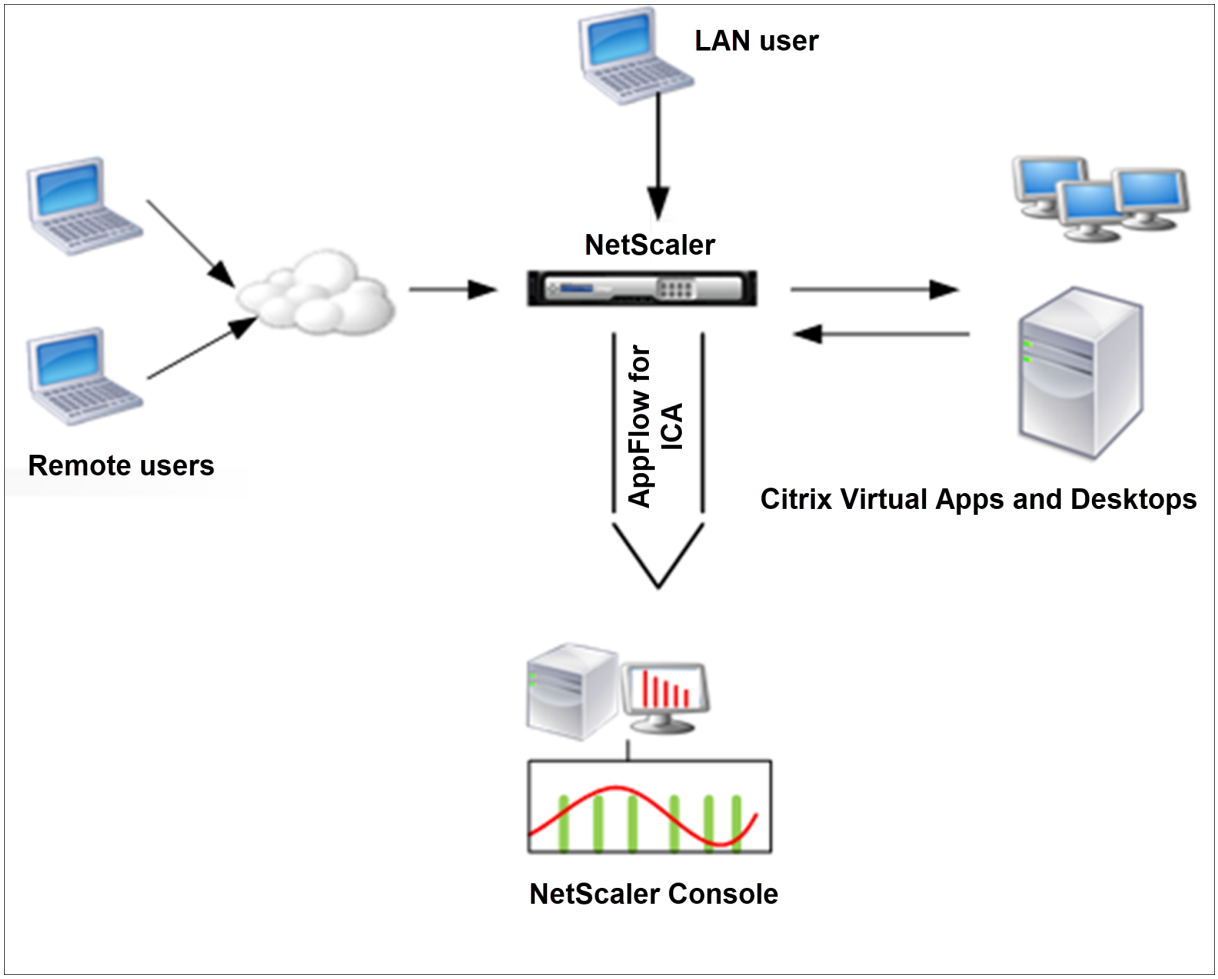
启用数据收集以监视在局域网用户模式下部署的 NetScaler

January 29, 2024

访问 Citrix 虚拟应用程序或桌面应用程序的外部用户必须在 NetScaler Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 NetScaler Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便请求重定向至 NetScaler 设备。

为了克服这些挑战，让局域网用户直接连接到 Citrix Virtual Apps and Desktops 应用程序，您可以通过配置缓存重定向虚拟服务器以局域网用户模式部署 NetScaler 设备。缓存重定向虚拟服务器充当 NetScaler Gateway 设备上的 SOCKS 代理。

下图说明了在局域网用户模式下部署的 **NetScaler** 控制台。



> 注意
>
> NetScaler Gateway 设备必须能够访问代理。

要监视在此模式下部署的 NetScaler 设备，请先将 NetScaler 设备添加到 NetScaler Insight 清单，启用 AppFlow，

然后在控制板上查看报告。

将 NetScaler 设备添加到 NetScaler 控制台清单后，必须启用 AppFlow 才能收集数据。

> 注意
>
> - 您无法使用 NetScaler 控制台配置实用程序在以局域网用户模式部署的 NetScaler 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅“命令参考”。
> - 有关策略表达式的信息，请参阅“策略和表达式”。

要使用命令行界面在 **NetScaler** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录到 NetScaler 设备。
2. 添加转发代理缓存重定向虚拟服务器并提供代理 IP 和端口，指定服务类型为 HDX。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
    cacheType <cachetype>] [ - cltTimeout <secs>]
```

示例：

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
    cltTimeout 180
```

> 注意
>
> 如果您使用 NetScaler Gateway 设备访问局域网网络，请添加操作以应用与 VPN 流量匹配的策略。

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

示例：

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. 在 NetScaler 设备上将 NetScaler 控制台添加为 AppFlow 收集器。

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
    \\>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
```


示例：

```
add appflow action act -collectors MyInsight
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

示例：

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
    type\>
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> 注
>
> 意 type 的值必须为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
```

示例：

```
set appflow param -flowRecordInterval 60
```

8. 保存配置。

```
save ns config
```

为 **HDX Insight** 创建阈值并配置警报

January 29, 2024

NetScaler 控制台上的 HDX Insight 允许您监视通过 NetScaler 实例的 HDX 流量。NetScaler 控制台允许您在用于监视 Insight 流量的各种计数器上设置阈值。您还可以在 NetScaler 控制台中配置规则和创建警报。

HDX 流量类型与各种实体（如应用程序、桌面、网关、许可证和用户）相关联。每个实体都可以包含与其关联的不同指标。例如，应用程序实体与多个命中、应用程序消耗的带宽和服务器的响应时间相关联。用户实体可以与用户使用的 WAN 延迟、DC 延迟、ICA RTT 和带宽相关联。

NetScaler 控制台中对 HDX Insight 的阈值管理允许您在违反设置的阈值时主动创建规则和配置警报。现在，此阈值管理已扩展到配置一组阈值规则。现在，您可以监视组而不是单个规则。阈值规则组由从用户、应用程序和桌面等实体中选择的指标的一个或多个用户定义的阈值规则组成。每个规则都会根据您在创建规则时输入的预期值进行监视。在用户实体中，阈值组也可以与地理位置关联。

仅当违反配置的阈值组中的所有规则时，才会在 NetScaler 控制台上生成警报。例如，您可以根据会话启动总数监视应用程序，也可以将应用程序启动计数作为一个阈值组进行监视。只有在违反两条规则时才会生成警报。这允许您在实体上设置更真实的阈值。

下面列出了几个示例：

- 阈值规则 1：用户（实体）的 ICA RTT（指标）必须 <= 100 毫秒
- 阈值规则 2：用户（实体）的 WAN 延迟（指标）必须 <= 100 毫秒

阈值组的示例可以是：{阈值规则 1 + 阈值规则 2}

要创建规则，必须首先选择要监视的实体。然后在创建规则时选择指标。例如，您可以选择应用程序实体，然后选择 会话启动总计数或应用程序启动计数。您可以为实体和指标的每种组合创建一条规则。使用提供的比较器（>、<、>= 和 <=），键入每个指标的阈值。

> 注意
>
> 如果您不想监视单个组中的多个实体，则必须为每个实体创建一个单独的阈值规则组。

当计数器的值超过阈值时，NetScaler 控制台会生成一个表示违反阈值的事件，并为每个事件创建警报。

您必须配置接收警报的方式。您可以启用在 NetScaler 控制台上显示警报，也可以通过电子邮件或两者同时接收警报，或者在移动设备上以 SMS 的形式接收警报。对于最后两项操作，必须在 NetScaler 控制台上配置电子邮件服务器或 SMS 服务器。

阈值组也可以绑定到地理位置，以便对用户实体进行特定地理监视。

用例示例

ABC Inc. 是一家全球性的公司，在 50 多个国家设有办事处。该公司有两个数据中心，一个位于新加坡，另一个位于加利福尼亚州，负责托管 Citrix Virtual Apps and Desktops。公司的员工使用 NetScaler Gateway 和基于 GSLB 的重定向在全球访问 Citrix Virtual Apps and Desktops。ABC 公司的 Citrix Virtual Apps and Desktops 管理员 Eric 希望跟踪其所有办公室的用户体验，以优化应用程序和桌面交付，随时随地访问。Eric 还希望检查用户体验指标，如 ICA RTT，延迟，并主动提出任何偏差。

ABC Inc. 的用户有一个分布式的存在。有些用户位于数据中心附近，有些用户位于远离数据中心的地方。随着用户群的分布广泛，指标和相应的阈值也因这些位置而异。例如，数据中心附近位置的 ICA RTT 可能为 5-10 毫秒，而远程位置的 ICA RTT 可能在 100 毫秒左右。

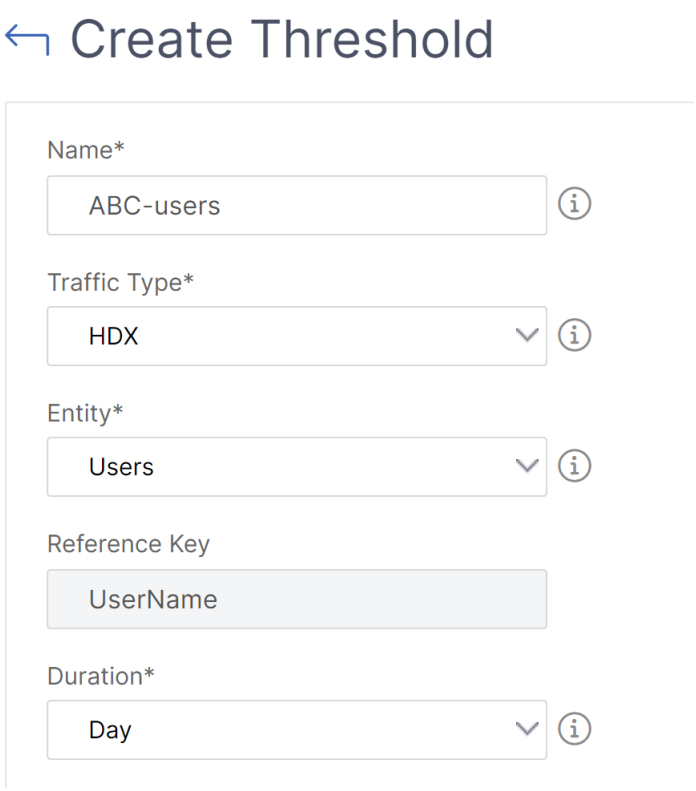
借助 HDX Insight 的阈值规则组管理，Eric 可以为每个位置设置特定地理位置的阈值规则组，并通过电子邮件或短信收到每个区域的违规警报。Eric 还能够将对阈值规则组中多个指标的跟踪结合起来，并将根本原因缩小到容量问题（如

果有)。Eric 现在能够主动跟踪任何偏差，而不必担心手动查看所有 Citrix Virtual Apps and Desktops 以获取 HDX Insight 产品组合指标的复杂性。

使用 **NetScaler** 控制台创建阈值规则组并为 **HDX Insight** 配置警报

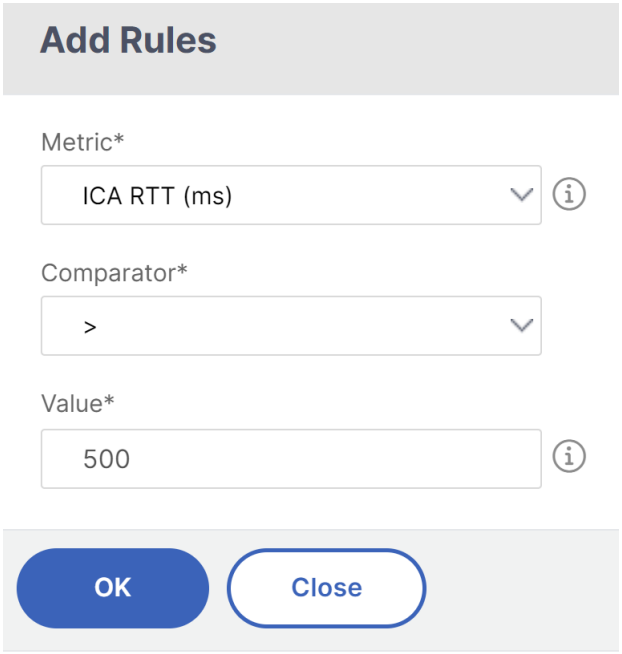
1. 在 NetScaler 控制台中，导航到“设置”**>**“分析设置”**>**“阈值”。在打开的阈值页面上，单击添加。
2. 在 **Create Thresholds and Alerts**（创建阈值和警报）页面上，指定以下详细信息：

   a) 名称。键入用于创建事件的名称，NetScaler 控制台会为该事件生成警报。
   b) 流量类型。从列表中选择 **HDX**。
   c) 实体。从列表中选择类别或资源类型。您之前选择的每种流量类型的实体不同。
   d) 参考键。参考密钥是根据您选择的流量类型和实体自动生成的。
   e) 持续时间。从列表中选择要监视实体的时间间隔。您可以监视实体一小时、一天或一周的持续时间。

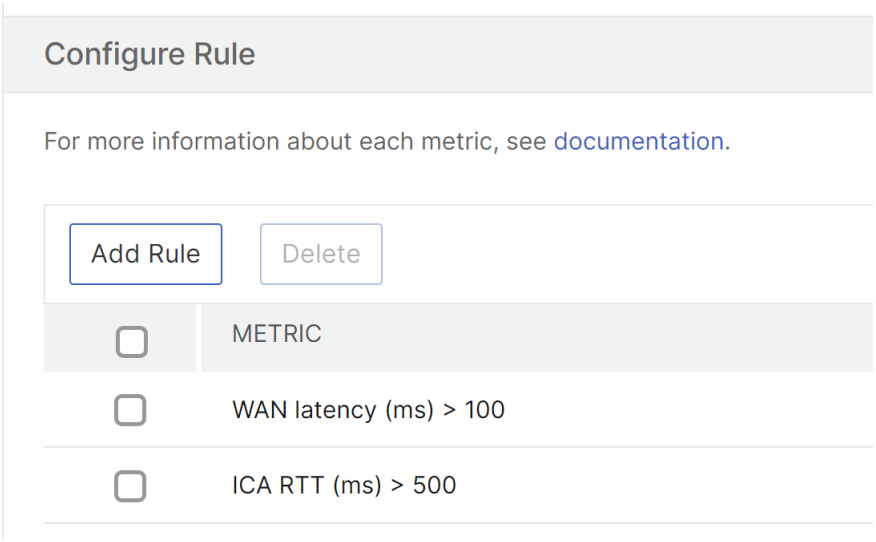


3. 为所有实体创建阈值规则组：

   对于 HDX 流量，必须通过单击“添加规则”来创建规则。在打开的“添加规则”弹出窗口中输入值。

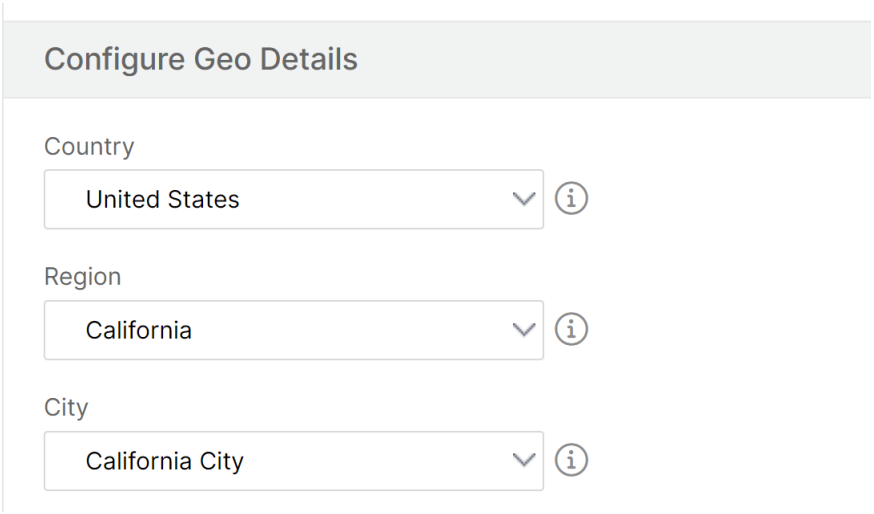


您可以创建多个规则来监视每个实体。在一个组中创建多个规则允许您将实体作为一组阈值规则而不是单个规则进行监视。单击确定关闭窗口。



4. 为用户实体配置地理位置标记：

   或者，您可以在“配置地理详细信息”部分中为用户实体创建基于位置的警报。下图显示了创建基于地理位置的标记以监视美国西海岸用户 WAN 延迟性能的示例。



5. 单击“启用阈值”以允许 NetScaler 控制台开始监视实体。
6. 或者，配置电子邮件和 Slack 通知等操作。
7. 单击创建以创建阈值规则组。

查看 **HDX Insight** 报告和指标

January 29, 2024

HDX Insight 提供与 NetScaler 实例上的 HDX 流量相关的报告和指标的完整可见性。

您可以查看任何选定实体的 HDX 指标。视图中包括以下类别的实体：

- 用户：显示在选定时间间隔内访问 Citrix Virtual Apps and Desktops 的所有用户的报告。
- 应用程序：显示应用程序总数的报告以及所有相关信息，例如应用程序在指定时间间隔内启动的总次数。
- 实例：显示用作传入流量网关的 NetScaler 实例的报告。
- 桌面：显示在选定时间范围内使用的桌面的报告。
- 许可证：显示指定时段内使用的 SSL VPN 许可证总数的报告。

本文档包括以下部分：

- “User”（用户）视图报告和指标
- “Application”（应用程序）视图报告和指标
- “Desktop”（桌面）视图报告和指标
- “Instance”（实例）视图报告和指标
- “License”（许可证）视图报告和指标

对 **HDX Insight** 问题进行故障排除

January 29, 2024

如果 HDX Insight 解决方案未按预期运行，则问题可能出在以下情况之一。有关故障排除，请参阅相应部分中的清单。

- HDX Insight 配置。
- NetScaler 和 NetScaler 控制台之间的连接。
- 在 NetScaler 中生成 HDX/ICA 流量的记录。
- NetScaler 控制台中的记录总量。

HDX Insight 配置清单

- 确保在 NetScaler 中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。
- 检查 NetScaler 运行配置中的 HDX Insight 配置。

  运行 `show running | grep -i <appflow_policy>` 命令以检查 HDX Insight 配置。确保绑定类型为 ICA 请求。例如;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  对于透明模式，绑定类型必须为 ICA_REQ_DEFAULT。例如;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- 对于单跃点/Access Gateway 或双跃点部署，请确保 HDX Insight AppFlow 策略绑定到 VPN 虚拟服务器，HDX/ICA 流量正在流动。
- 对于透明模式或局域网用户模式，请确保设置 ICA 端口 1494 和 2598。
- 已为 Access Gateway 或双跃点部署启用 NetScaler Gateway 或 VPN 虚拟服务器中的检查 `appflowlog` 参数。有关详细信息，请参阅 为虚拟服务器启用 AppFlow。
- 选中双跃点 NetScaler 中已启用“连接链接”。有关详细信息，请参阅 配置 NetScaler Gateway 设备以导出数据。
- HA 故障转移后，如果 HDX Insight 详细信息被跳过解析，请检查 ICA 参数“enableSRonHAFailover”是否已启用。有关详细信息，请参阅 NetScaler 高可用性对上的会话可靠性。

NetScaler 和 **NetScaler** 控制台之间的连接清单

- 检查 NetScaler 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 NetScaler 和 AppFlow Collector 之间的连接状态。

- 检查 HDX Insight AppFlow 策略命中。

  运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中情况。

  您还可以导航到 GUI 中的“系统”**>**“**AppFlow**”**>**“策略”，以检查 AppFlow 策略命中。

- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

在 **NetScaler** 核对表中为 **HDX/ICA** 流量生成记录

运行命令 `tail -f /var/log/ns.log | grep -i "default ICA Message"` 进行日志验证。根据生成的日志，您可以使用此信息进行故障排除。

- 日志：跳过解析 **ICA** 连接 **-** 此主机不支持 **HDX Insight**

  原因：Citrix Virtual Apps and Desktops 版本不受支持

  解决办法：将 Citrix Virtual Apps and Desktops 服务器升级到受支持的版本。

- 日志：**Client type received 0x53, NOT SUPPORTED**

  原因：Citrix Workspace 应用程序版本不受支持

  解决方案：将 Citrix Workspace 应用程序升级到受支持的版本。有关详细信息，请参阅 Citrix Workspace 应用程序。

- 日志：来自扩展数据包的错误-跳过此流的所有 **hdx** 处理

  原因：解压缩 ICA 流量时出现问题

  解决方案：在建立新会话之前，此 ICA 会话没有可用的报告。

- 日志：无效过渡：**NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT**

  原因：解析 ICA 握手时出现问题

  解决方案：在建立新会话之前，此特定 ICA 会话没有可用的报告。

- 日志：缺少 **EUEM ICA RTT**

  原因：无法解析最终用户体验监视通道数据

  解决方案：确保在 Citrix Virtual Apps and Desktops 服务器上启动了最终用户体验监视服务。确保您使用的是受支持的 Citrix Workspace 应用程序版本。

- 日志：通道标头无效

  原因：无法识别通道头

  解决方案：在建立新会话之前，此特定 ICA 会话没有可用的报告。

- 日志：跳过代码

  如果您看到以下任何跳过代码值，则会跳过解析 Insight 详细信息。

> 跳过代码 0 表示记录已成功从 NetScaler 导出。

跳过代码	错误消息	错误原因
100	NS_ICA_ERR_NULL_FRAG	处理 ICA 碎片时出错，可能是内存状况造成的
101	NS_ICA_ERR_INVALID_HS_CMD	收到的握手命令无效
102	NS_ICA_ERR_REDUC_PARAM_CNT	为 V3 扩展器初始化指定的参数无效
103	NS_ICA_ERR_REDUC_INIT	无法正确初始化 V3 扩展器
104	NS_ICA_ERR_REDUC_PARAM_BYTES	字节不足，无法将编码器分配给通道
105	NS_ICA_ERR_INVALID_CHANNEL	ICA 通道号无效
106	NS_ICA_ERR_INVALID_DECODER	为通道指定的解码器无效
107	NS_ICA_ERR_INVALID_TW_PARAM	在 Thinwire 通道上指定的参数计数无效
108	NS_ICA_ERR_INVALID_TW_DECODER	Thinwire 通道的解码器无效
109	NS_ICA_ERR_REDUC_NO_DECODER	没有为通道定义解码器
110	NS_ICA_ERR_REDUC_V3_EXPANDER	无法扩展通道数据
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	V3 扩展器错误：消耗的字节多于可用字节
112	NS_ICA_ERR_REDUC_BYTES_OOR	错误：未压缩的数据溢出
113	NS_ICA_ERR_REDUC_INVALID_CMD	未定义的扩展器命令
114	NS_ICA_ERR_CGP_FILL_HOLE	处理拆分 CGP 帧时出错
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB 分配错误—由于内存不足
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	扩展器上下文的内存分配错误
117	NS_ICA_ERR_ICA_OLD_SERVER	旧服务器，不支持功能块
118	NS_ICA_ERR_PIR_MANY_FRAG	数据包初始化请求被分段，无法处理
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 功能初始化错误
120	NS_ICA_ERR_NO_MSI_SUPPORT	主机不支持 MSI 功能。表示低于 6.5 的 XenApp 版本或低于 5.0 的 XenDesktop 版本
121	NS_ICA_ERR_CGP_INVALID_CMD	遇到无效的 CGP 命令
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	通道上的字节数不足

跳过代码	错误消息	错误原因
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL 或 SEAMLESS 通道上的数据不正确
124	NS_ICA_ERR_INVALID_PURE_CMD	处理 PURE ICA 通道数据时收到无效命令
125	NS_ICA_ERR_INVALID_PURE_LEN0	处理 PURE ICA 通道数据时遇到无效长度
126	NS_ICA_ERR_INVALID_PURE_LEN	处理 PURE ICA 通道数据时遇到无效长度
127	NS_ICA_ERR_INVALID_CLNT_DATA	从客户端接收到的数据长度无效
128	NS_ICA_ERR_MSI_GUID_SZ	MSI GUID 大小错误
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	检测到无效的通道头
130	NS_ICA_ERR_CGP_PARSE_RECONNECT	在 CGP 重新连接的会话失败
131	NS_ICA_ERR_DISABLE_SR_NON_MSRDP_CONNECT	禁用 SR 非 MSRDP 连接
132	NS_ICA_ERR_REDUC_NOT_V3	不支持的 ICA Reducer 版本
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	已禁用压缩，主机不支持压缩
134	NS_ICA_ERR_IDENT_PROTO	无法识别 ICA 或 CGP 协议，接收器不正确
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 签名或幻字符串不正确
136	NS_ICA_ERR_PARSE_RAW	解析 ICA 握手数据包时出错
137	NS_ICA_ERR_INCOMPLETE_PKT	握手时收到的数据包不完整
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA 帧太大，超过 1,460 字节
139	NS_ICA_ERR_FORWARD	转发 ICA 数据时出错
140	NS_ICA_ERR_MAX_HOLES	无法处理 CGP 命令，因为它被拆分超出了支持的限制
141	NS_ICA_ERR_ASSEMBLE_FRAME	无法正确重组 ICA 框架
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	已跳过此 ICA（客户端）的 ICA 解析，因为它不在允许列表中
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	无法检测客户端重新连接 Cookie 的解析状态
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	客户端重新连接后检测到的重新连接 Cookie 长度无效
145	NS_ICA_ERR_INVALID_RECONNECT_ID	客户端重新连接 cookie 错过了所需的约束

跳过代码	错误消息	错误原因
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	从客户端收到的 Workspace 版本字符串无效
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	从客户端收到的产品编码无效
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	压缩后的通道长度无效
149	NS_ICA_ERR_SPECIAL_THINWIRE	解压缩错误
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	遇到无法执行无缝命令的字节不足的问题
151	NS_ICA_ERR_EUEM_INSUFFBYTE	遇到 EUEM 命令的字节不足
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	无缝通道解析的事件无效
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRL 通道解析的事件无效
154	NS_ICA_ERR_EUEM_INVALID_EVENT	EUEM 通道解析的事件无效
155	NS_ICA_ERR_USB_INVALID_EVENT	USB 通道解析的事件无效
156	NS_ICA_ERR_PURE_INVALID_EVENT	PT 通道解析的事件无效
157	NS_ICA_ERR_VCP_INVALID_EVENT	虚拟通道解析的事件无效
158	NS_ICA_ERR_ICAP_INVALID_EVENT	ICA 数据解析的事件无效
159	NS_ICA_ERR_CGPP_INVALID_EVENT	CGP 数据解析的事件无效
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	基本加密中 crypt 命令的状态无效
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	基本加密中 crypt 命令无效
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	RC5 加密中 crypt 命令的状态无效
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	RC5 加密中的 crypt 命令无效
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5 加密/解密时出错
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5 加密/解密时出错
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA 不支持 Reducer 版本 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace 不支持 Reducer 版本 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICA 握手中出现意外的字节数
169	NS_ICA_ERR_HIGHER_RECONSEQ	对等发布重新连接的 CGP 恢复序列号较高
170	NS_ICA_ERR_DESCSRINFO_ABSENT	重新连接后无法恢复 ICA 解析状态
171	NS_ICA_ERR_NSAP_PARSING	解析 Insight 通道数据时出错

跳过代码	错误消息	错误原因
172	NS_ICA_ERR_NSAP_APP	从 Insight 渠道数据解析应用详细信息时出错
173	NS_ICA_ERR_NSAP_ACR	解析 Insight 通道数据中的 ACR 详细信息时出错
174	NS_ICA_ERR_NSAP_SESSION_END	从 Insight 通道数据解析会话结束详细信息时出错
175	NS_ICA_ERR_NON_NSAP_SN	由于缺少 Insight 渠道支持，跳过了服务节点上的 ICA 解析
176	NS_ICA_ERR_NON_NSAP_CLIENT	客户端不支持 NSAP
177	NS_ICA_ERR_NON_NSAP_SERVER	VDA 不支持 NSAP
178	NS_ICA_ERR_NSAP_NEG_FAIL	NSAP 数据协商时出错
179	NS_ICA_ERR_SN_RECONNECT_TKT	获取服务节点中的票证
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	从服务节点中接收更高的重新连接序列号时出错
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONSAP	为非 NSAP 连接禁用 HDX Insight 时出错

示例日志：

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
 ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
 send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
 Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"

Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
 [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```


错误计数器

ICA 解析时会捕获各种计数器。下表列出了用于 ICA 解析的各种计数器。
运行命令 `nsconmsg -g hdx -d statswt0` 查看计数器详细信息。

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_tot_ica_conn	指示 NS 检测到的纯 ICA 连接的总数。每当检测到基于客户端 PCB 上的 ICA 签名的 ICA 连接时，就会递增。	统计信息
hdx_tot_cgp_conn	指示 NS 检测到的 CGP 连接总数（会话可靠性开启）。每当检测到基于客户端 PCB 上的 CGP 签名的 CGP 连接时，就会递增。	统计信息
hdx_dbg_tot_udt_conn	表示 NS 检测到的 UDP ICA 连接总数	统计信息
hdx_dbg_tot_nsap_conn	表示 NS 检测到的支持 NSAP 的连接总数	统计信息
hdx_tot_skip_conn	表示由于 ICA 或 CGP 签名无效，解析器跳过了多少个 ICA 连接。	统计信息
hdx_dbg_active_conn	当时活跃的 EDT/CGP/ICA 连接总数。	统计信息
hdx_dbg_active_nsap_conn	当时活跃的 EDT/CGP/ICA NSAP 连接总数。	统计信息
hdx_dbg_skip_appflow_disabled	由于禁用 AppFlow 而将 AppFlow 从会话中分离的实例总数	统计/诊断
hdx_dbg_transparent_user	透明用户访问的总数	统计/诊断
hdx_dbg_ag_user	Access Gateway 用户访问总数	统计/诊断
hdx_dbg_lan_user	局域网用户模式访问总数	统计/诊断
hdx_basic_enc	指示使用基本加密的 ICA 连接数	统计/诊断
hdx_advanced_enc	表示使用基于 RC5 的高级加密的 ICA 连接数	统计/诊断
hdx_dbg_reconnected_session	来自客户端的未出现任何 NetScaler 错误的重新连接请求总数	统计/诊断
被拒绝的主机重新连接	客户端拒绝的重新连接请求的主机总数	统计/诊断
hdx_euem_available	指示具有“最终用户体验监视”通道可用的连接数。需要使用最终用户体验监视通道来收集 ICA RTT 等统计信息。	统计/诊断

HDX 计数器名称	用途	类别（统计/错误/诊断）
已禁用的高清错误	使用 nsapimgr 旋钮禁用会话可靠性。会话不适用于此会话。	错误
hdx_err_skip_no_msi	XA/XD 服务器缺少 MSI 功能。这表示服务器版本较旧，HDX Insight 会跳过此连接。	错误
hdx_err_skip_old_server	不支持的旧服务器版本	错误
高清错误白名单	客户端接收器不在允许列表中，HDX Insight 会跳过此连接	错误
hdx_sm_ica_cam_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CAM_CHANNEL 总数	诊断
hdx_sm_ica_usb_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_USB_CHANNEL 总数	诊断
hdx_sm_ica_clip_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CLIP_CHANNEL 总数	诊断
hdx_sm_ica_ccm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CCM_CHANNEL 总数	诊断
hdx_sm_ica_cdm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CDM_CHANNEL 总数	诊断
hdx_sm_ica_com1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM1_CHANNEL 总数	诊断
hdx_sm_ica_com2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM2_CHANNEL 总数	诊断
hdx_sm_ica_cpm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CPM_CHANNEL 总数	诊断
hdx_sm_ica_lpt1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT1_CHANNEL 总数	诊断
hdx_sm_ica_lpt2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT2_CHANNEL 总数	诊断
dx_dbg_sm_ica_msi_disabled	通过 SmartAccess 策略禁用 MSI 的案例总数	诊断
hdx_sm_ica_file_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_FILE_CHANNEL 总数	诊断
hdx_dbg_usb_accept_device	接受的 USB 设备总数	诊断
hdx_dbg_usb_reject_device	拒绝的 USB 设备总数	诊断
hdx_dbg_usb_reset_endpoint	重置的 USB 端点总数	诊断
hdx_dbg_usb_reset_device	重置的 USB 设备总数	诊断

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_dbg_usb_stop_device	已停止的 USB 设备总数	诊断
hdx_dbg_usb_stop_device_response	来自已停止的 USB 设备的响应总数	诊断
hdx_dbg_usb_device_gone	消失的 USB 设备总数	诊断
hdx_dbg_usb_device_stopped	已停止的 USB 设备总数	诊断

nstrace validation

检查 CFLOW 协议以查看 NetScaler 中的所有 AppFlow 记录。

NetScaler 控制台清单中的记录总量

- 运行该`tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record : ica_"`命令 并检查日志，以确认 NetScaler 控制台正在接收 AppFlow 记录。
- 确认已将 NetScaler 实例添加到 NetScaler 控制台。
- 验证 NetScaler Gateway/VPN 虚拟服务器是否已在 NetScaler 控制台中获得许可。
- 确保为双跃点启用了多跳参数设置。
- 确保 NetScaler Gateway 在双跃点部署中已获得第二跃点许可。

在联系 Citrix 技术支持之前

要快速解决问题，请确保在联系 Citrix 技术支持之前已掌握以下信息：

- 部署和网络拓扑的详细信息。
- NetScaler 和 NetScaler 控制台版本。
- Citrix Virtual Apps and Desktops 服务器版本。
- 客户端 Workspace 版本。
- 发生问题时的活动 ICA 会话数。
- 通过在 NetScaler `show techsupport` 命令提示符下运行命令捕获的技术支持包。
- 为 NetScaler 控制台捕获的技术支持包。
- 在所有 NetScaler 上捕获的数据包跟踪。
  要启动数据包跟踪，请键入，`start nstrace -size 0'`
  要停止数据包跟踪，请键入、`stop nstrace`

- 通过运行 `show arp` 命令收集系统 ARP 表中的条目。

已知问题

有关 HDX Insight 的已知问题，请参阅 NetScaler 发行说明。

阈值的指标信息

January 29, 2024

您可以创建阈值，并在阈值突破时收到通知。在典型部署中，您可以将阈值设置为：

- 跟踪各种应用程序指标
- 促进规划
- 每当应用程序的指标值超过设定的阈值时都会收到通知

要配置阈值：

1. 导航到设置 **>** 分析设置 **>** 阈值。
2. 在“阈值”页上，单击“添加”。

Web

指标	实体	说明
应用程序	访问量	虚拟服务器（应用程序）收到的点击总数
	带宽 (MB)	虚拟服务器（应用程序）消耗的总带宽
	响应时间（毫秒）	虚拟服务器响应所花费的时间
客戶端	请求	客户端收到的请求总数
	渲染时间 (毫秒)	客户端呈现服务器响应所花费的时间
	客户端网络延迟	来自客户端网络的请求所花费的时间
设备	访问量	设备收到的点击总数。例如：笔记本电脑、手机
	带宽 (MB)	设备消耗的总带宽
域	访问量	网络域收到的命中总数

指标	实体	说明
	带宽 (MB)	网络域消耗的总带宽
	响应时间（毫秒）	响应网络域请求所花费的时间
操作系统	访问量	操作系统收到的点击总数
	带宽 (MB)	操作系统消耗的总带宽
	渲染时间 (毫秒)	操作系统呈现服务器响应所花费的时间
请求方法	访问量	通过请求方法接收的请求总数。例如：GET、POST
	带宽 (MB)	请求方法消耗的总带宽
答复状态	访问量	收到的带有响应代码的点击总数
	带宽 (MB)	响应代码消耗的总带宽
服务器	访问量	服务器收到的请求/点击总数
	带宽 (MB)	服务器消耗的总带宽
	服务器网络延迟 (ms)	来自服务器网络的请求所花费的时间
	服务器处理时间 (ms)	服务器响应请求所花费的时间
URL	访问量	URL 收到的点击总数。例如：www.Citrix.com
	加载时间 (ms)	从服务器加载 URL 所花费的时间
	渲染时间 (毫秒)	URL 呈现和显示所花费的时间
用户代理	访问量	用户代理收到的请求总数。例如：Chrome 网络浏览器
	带宽 (MB)	用户代理消耗的总带宽
	渲染时间 (毫秒)	用户代理呈现服务器响应所花费的时间

安全性

指标	实体	说明
应用程序	Threat Index（威胁指数）	一个单位数评级系统，用于指示应用程序攻击的严重程度。应用程序上的攻击越严重，该应用程序的威胁指数越高。值范围介于 1 到 7 之间。
	安全指数	一个单位数评级系统，用于指示您配置 NetScaler 实例以保护应用程序免受外部威胁和漏洞的安全性。应用程序的安全风险越低，安全指数越高。值范围介于 1 到 7 之间。

APPANALYTICS

指标	实体	说明
应用程序	AppScore	App Score 定义应用程序的性能如何，并显示该应用程序在响应能力方面是否表现良好。值范围为 0 到 80。

HDX

有关 HDX 阈值的信息，请参阅为 HDX Insight 创建阈值和配置警报

基础结构分析

March 10, 2024

网络管理员的一个关键目标是监视 NetScaler 实例。NetScaler 实例为通过它访问的应用和桌面的使用和性能提供了有趣的见解。管理员必须监视 NetScaler 实例并分析每个 NetScaler 实例处理的应用程序流。管理员还必须能够修复配置、设置、连接、证书方面的任何可能问题以及对应用程序使用或性能的其他影响。例如，应用程序流量模式的突然变化可能是由于 SSL 配置的更改（例如禁用 SSL 协议）造成的。管理员必须能够快速识别这些数据点之间的关联，以确保以下几点：

- 应用程序可用性处于最佳状态
- 不存在资源消耗、硬件、容量或配置更改问题
- 没有未使用的库存

- 没有过期的证书

基础结构分析功能通过关联多个数据源并量化为定义实例运行状况的可衡量得分，简化了数据分析流程。借助此功能，管理员可以通过单一接触点了解问题、问题的根源以及他们可以采取的可能的补救措施。

NetScaler 控制台中的基础架构分析

基础设施分析功能整理从 NetScaler 实例收集的所有数据，并将其量化为定义 实例运行状况的实例得分。实例得分通过表格视图或以圆形包可视化形式进行汇总。基础结构分析功能可帮助您可视化导致或可能导致实例问题的因素。此可视化还可以帮助您确定为防止问题及其再次出现而必须执行的操作。

实例得分

实例评分表示 NetScaler 实例的运行状况。得分为 100 表示实例运行状况良好，没有任何问题。实例得分可捕捉实例上不同级别的潜在问题。它是实例运行状况的可量化衡量标准，多个“运行状况指标”为得分做出了贡献。

运行状况指标 是实例得分的基石，在实例得分中，根据在该时间窗口内检测到的所有指标，定期计算预定义的“监视周期”的得分。目前，基础设施分析根据从实例收集的数据每小时计算一次实例得分。
指标可以定义为属于实例上以下类别之一的任何活动（事件或问题）。

- 系统资源指示器
- 关键事件指标
- SSL 配置指示器
- 配置偏差指示器

运行状况指标解释

- 系统资源指标

  以下是可能在 NetScaler 实例上发生并由 NetScaler 控制台监视的关键系统资源问题。

  - **CPU** 使用率高。在 NetScaler 实例中，CPU 使用率已超过较高的阈值。
  - 内存使用率高。在 NetScaler 实例中，内存使用量已超过较高的阈值。
  - 磁盘使用率高。在 NetScaler 实例中，磁盘使用量已超过较高的阈值。
  - 磁盘错误。安装了 NetScaler 实例的虚拟机管理程序上的硬盘 0 或硬盘 1 上出现错误。
  - 电源故障。电源出现故障或与 NetScaler 实例断开连接。
  - **SSL** 卡出现故障。安装在实例上的 SSL 卡出现故障。
  - 闪存错误。在 NetScaler 实例上看到紧凑型闪存错误。

- 网卡丢弃。NIC 卡丢弃的数据包已跨越 NetScaler 实例中较高的阈值。

有关这些系统资源错误的更多信息，请参阅 实例控制板。

- 关键事件指标

  以下关键事件由配置为严重性的 NetScaler 控制台事件管理功能下的事件标识。

  - **HA** 同步失败。辅助服务器上处于高可用性状态的 NetScaler 实例之间的配置同步失败。
  - 哈哈没有心跳。一对处于高可用性的 NetScaler 实例中的主服务器无法接收来自辅助服务器的心跳。
  - **HA** 次要状态不正确。一对处于高可用性的 NetScaler 实例中的辅助服务器处于关闭、未知或保持辅助状态。
  - **HA** 版本不匹配。安装在一对 NetScaler 实例上的高可用性版本的 NetScaler 软件镜像版本不匹配。
  - 群集同步失败。群集模式下的 NetScaler 实例之间的配置同步失败。
  - 群集版本不匹配。以群集模式安装在 NetScaler 实例上的 NetScaler 软件映像版本不匹配。
  - 群集传播失败。向群集中的所有实例传播配置已失败。

    > 注意：
    >
    > 您可以通过更改事件的严重性级别来获得关键 SNMP 事件的列表。有关如何更改严重性级别的更多信息，请参阅 修改 NetScaler 实例上发生的事件的报告严重性。

  有关 NetScaler 控制台中事件的更多信息，请参见事件。

- SSL 配置指示器

  - 不建议密钥强度。SSL 证书的密钥强度不符合 NetScaler 标准
  - 不建议发行人。Citrix 不建议使用 SSL 证书的颁发者。
  - **SSL** 证书已过期。安装在 NetScaler 实例中的 SSL 证书已过期。
  - **SSL** 证书到期。安装在 NetScaler 实例中的 SSL 证书即将在未来一周内过期。
  - 不建议算法。安装在 NetScaler 实例中的 SSL 证书的签名算法不符合 NetScaler 标准。

有关 SSL 证书的更多信息，请参阅 SSL 控制板。

- 配置偏差指示器

  - 配置漂移模板。您使用要对某些实例进行审核的特定配置创建的审核模板存在配置偏差（未保存的更改）。
  - 配置偏移默认。默认配置文件中的配置存在偏移（未保存的更改）。

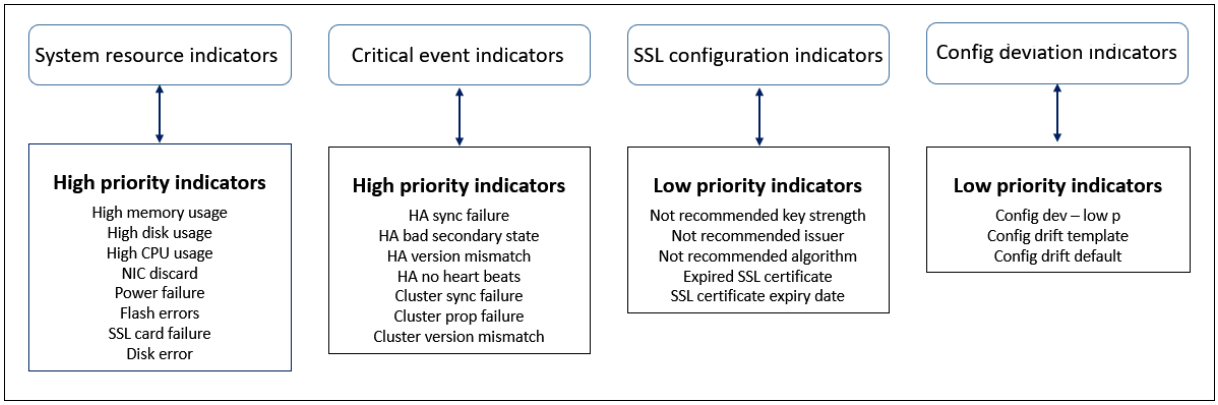
有关配置偏差以及如何运行审核报告来检查配置偏差的更多信息，请参阅 [查看审核报告]。(/en-us/netscaler-console-service/networks/configuration-audit/audit-reports.html)。

查看 **NetScaler** 容量问题

当 NetScaler 实例消耗了其大部分可用容量时，在处理客户端流量时可能会丢包。通过了解此类的 NetScaler 容量问题，您可以主动分配额外的许可来稳定 NetScaler 性能。有关更多信息，请参见 查看 NetScaler 实例中的容量问题。

运行状况指标的价值

这些指标根据以下价值分为高优先指标和低优先指标：



同一组指标中的运行状况指标具有不同的权重。一个指标可能比另一个指标更能降低实例得分。例如，高内存使用率比高磁盘使用率、高 CPU 使用率和 NIC 丢弃更能降低实例得分。如果在实例上检测到的指标数量较多，则实例得分越低。

指标的值是根据以下规则计算的。据说该指标可以通过以下三种方式之一进行检测：

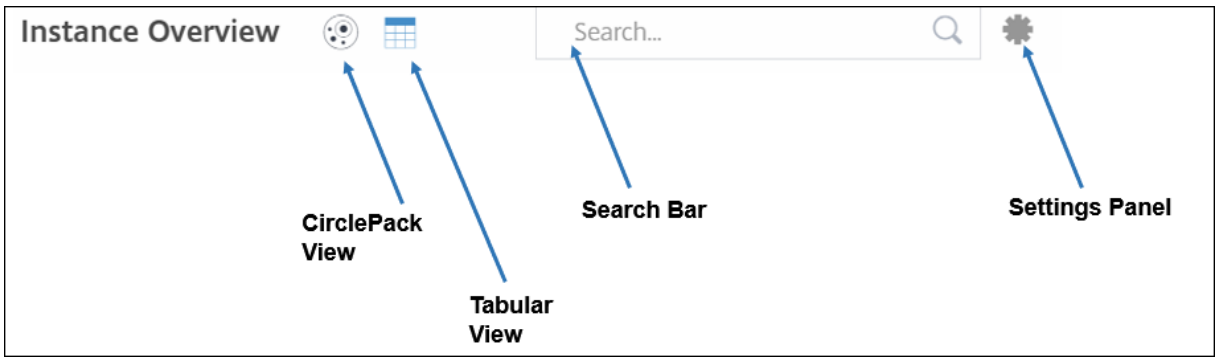
1. 基于某项活动。例如，每当实例出现电源故障时，系统资源指示器就会触发，该指示器会降低实例得分的值。当指标被清除时，惩罚被清除，实例得分增加。
2. 根据阈值突破情况而定。例如，当 NIC 卡丢弃数据包并且超过阈值级别时，会触发系统资源指示器。
3. 基于低阈值和高阈值突破情况。在这里，可以通过两种方式触发指标：
    - 当指标的值介于低阈值和高阈值之间时，将对实例得分征收部分罚款。
    - 当该值超过上限阈值时，将对实例得分征收全额罚款。
    - 如果该值降至低阈值以下，则不会对实例得分征收任何罚款。

例如，CPU 使用率是当使用率值超过低阈值时触发的系统资源指示器，也是在该值超过高阈值时触发的系统资源指标。

基础设施分析控制板

导航到 基础结构 **>** 基础结构分析。

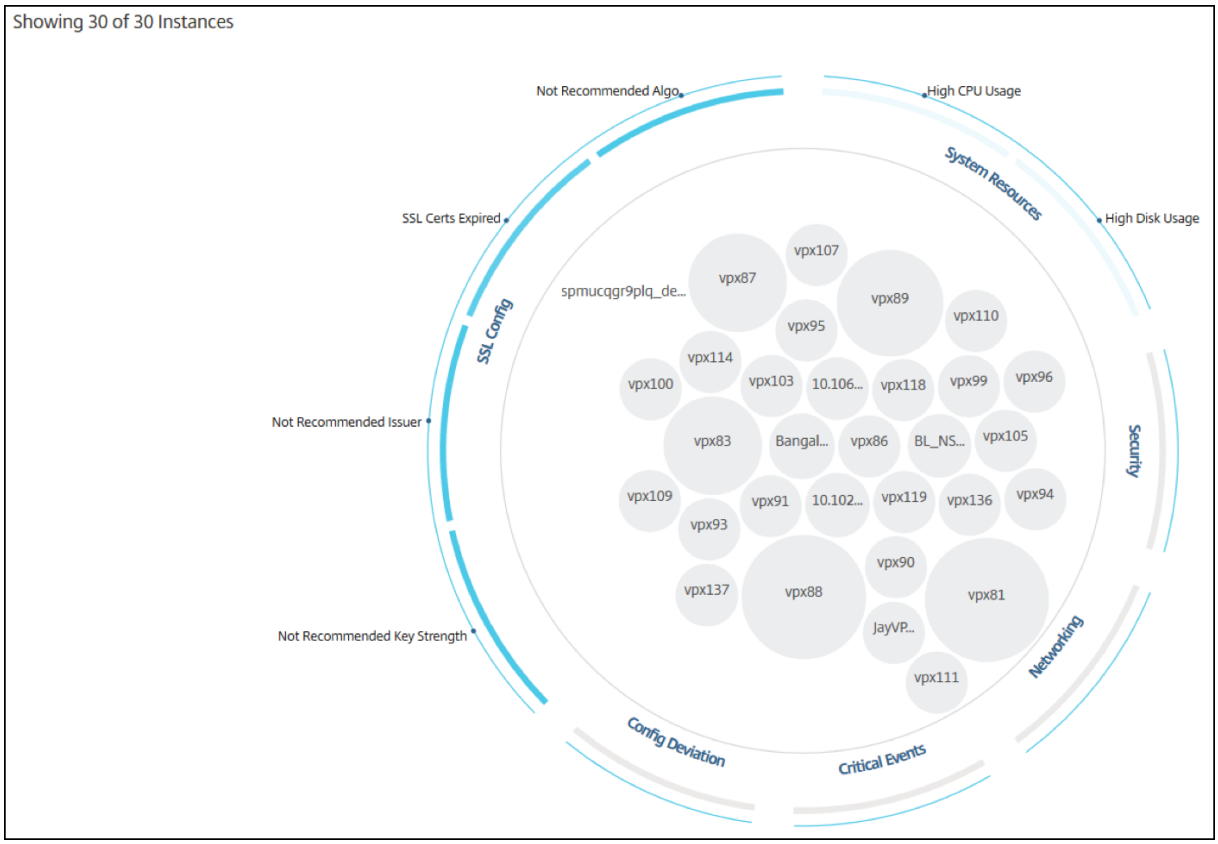
基础设施分析可以通过 圆形包 格式或 表格格 式查看。您可以在两种格式之间切换。



- 在“表格”视图中，您可以通过在搜索栏中键入主机名或 IP 地址来搜索实例。
- 默认情况下，基础设施分析页面在页面的右侧显示摘要面板。
- 单击“设置”图标以显示“设置”面板。
- 在这两种视图格式中，摘要面板显示网络中所有实例的详细信息。

圈子包视图

圆形包装图将实例组显示为组织严密的圆圈。它们通常显示层次结构，其中较小的实例组要么颜色与同一类别中的其他实例组相似，要么嵌套在较大的组中。圆包表示分层数据集，并显示层次结构中的不同级别以及它们之间的交互方式。



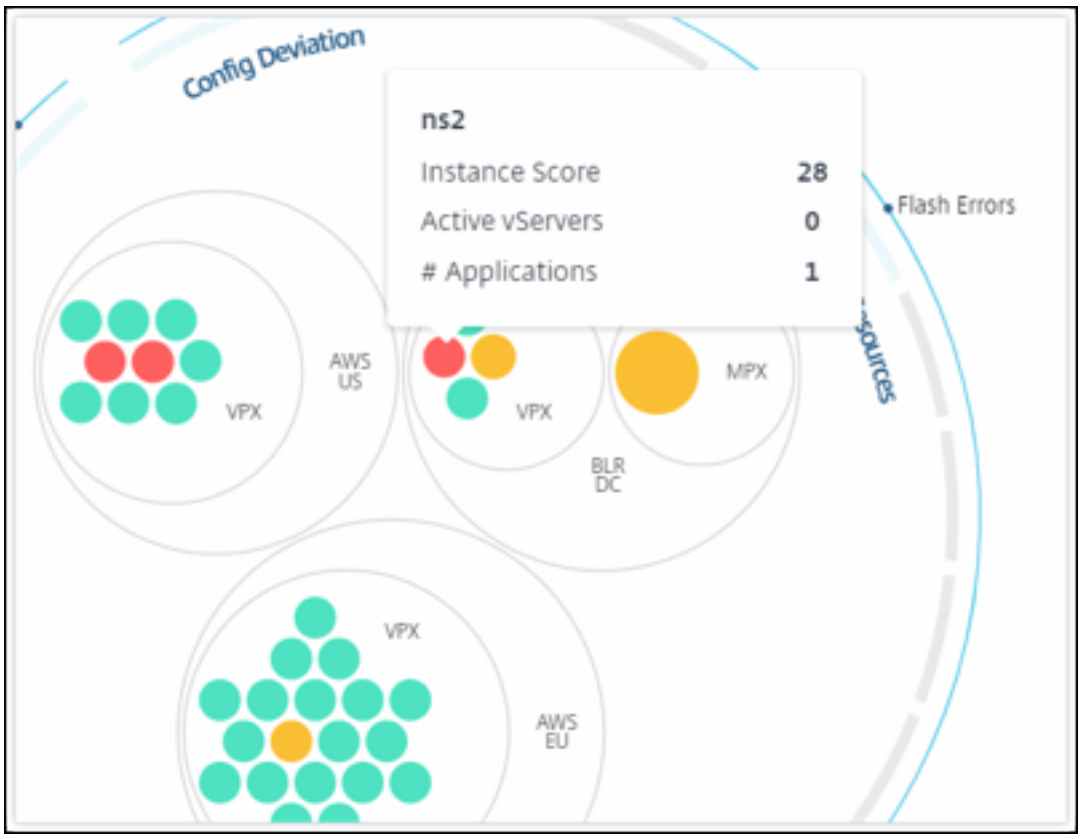
实例圆

颜色。每个实例在 Circle Pack 中都表示为彩色圆圈。圆圈的颜色表示该实例的运行状况。

- 绿色 -实例得分介于 100 和 80 之间。该实例运行正常。
- 黄色 -实例得分介于 80 到 50 之间。已经注意到一些问题，需要审查。
- 红色 -实例得分低于 50。该实例处于关键阶段，因为在该实例上发现了多个问题。

大小。这些彩色圆圈的大小表示在该实例上配置的虚拟服务器的数量。圆圈越大，表示虚拟服务器的数量越多。

您可以将鼠标指针悬停在每个实例圆圈（彩色圆圈）上以查看摘要。悬停工具提示显示实例的主机名、活动虚拟服务器的数量和在该实例上配置的应用程序数量。

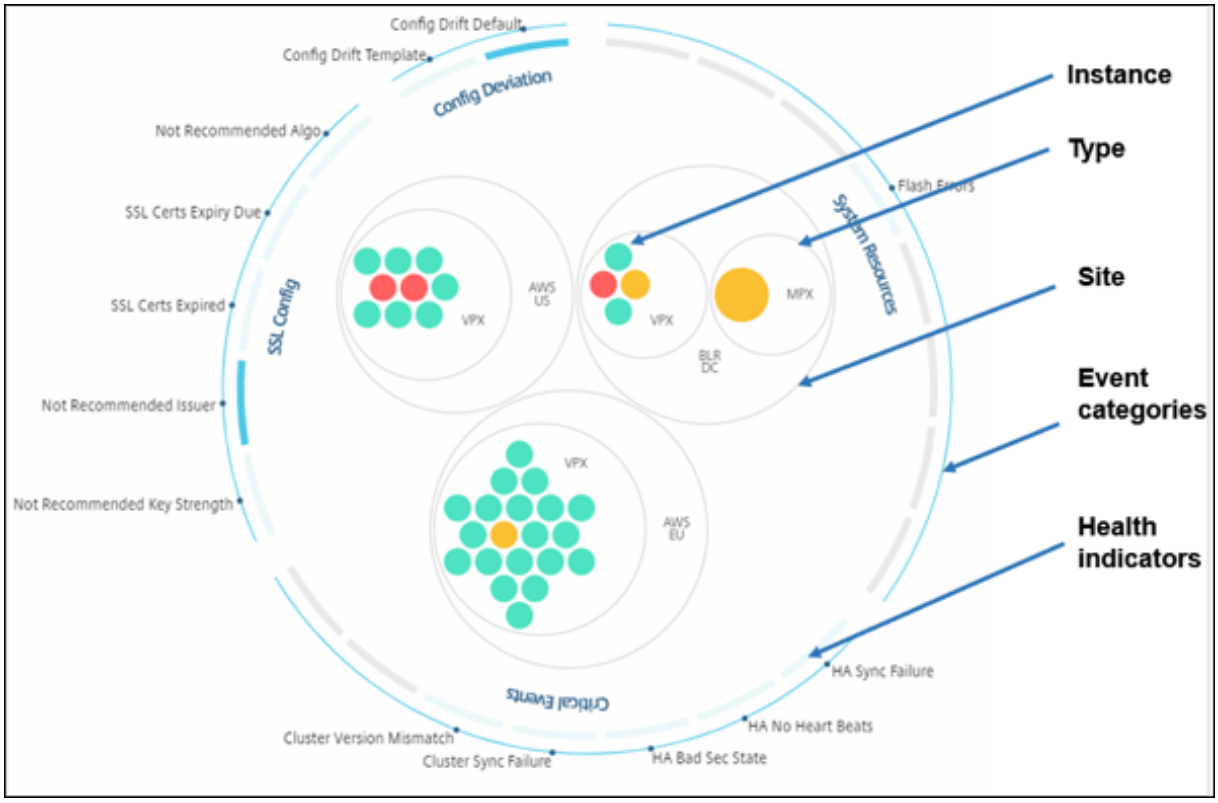


分组实例圆

Circle Pack 从一开始就由实例圈组成，这些圈子根据以下标准分组、嵌套或打包在另一个圈子中：

- 部署它们的站点
- 部署的实例类型-VPX、MPX、SDX 和 CPX
- NetScaler 实例的虚拟或物理模型
- 安装在实例上的 NetScaler 镜像版本

下图显示了 Circle Pack，其中实例首先按部署实例的站点或数据中心进行分组，然后根据实例的类型 VPX 和 MPX 进一步分组。

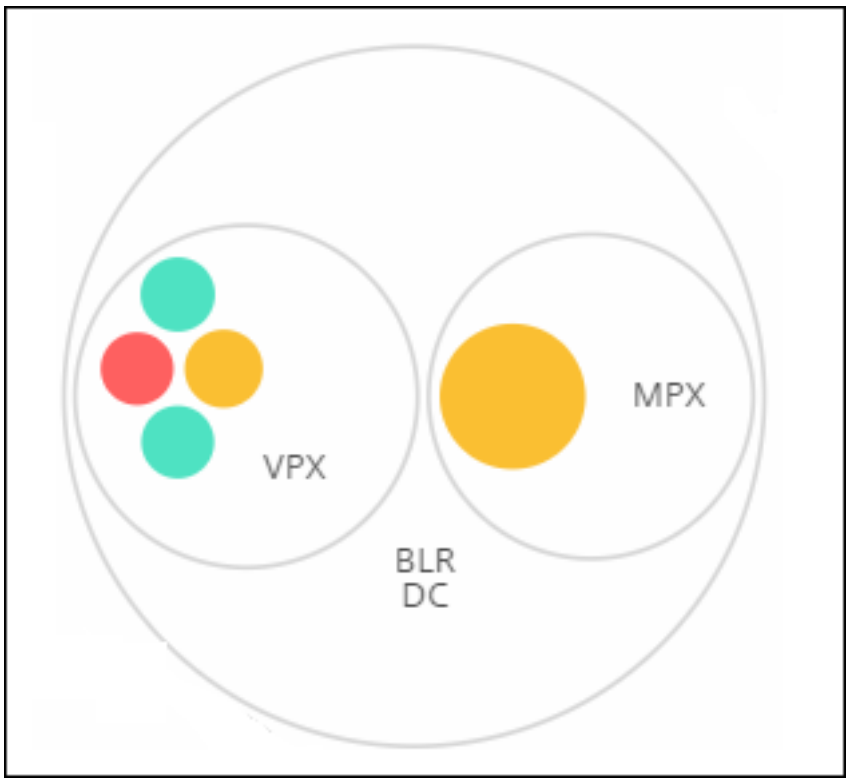


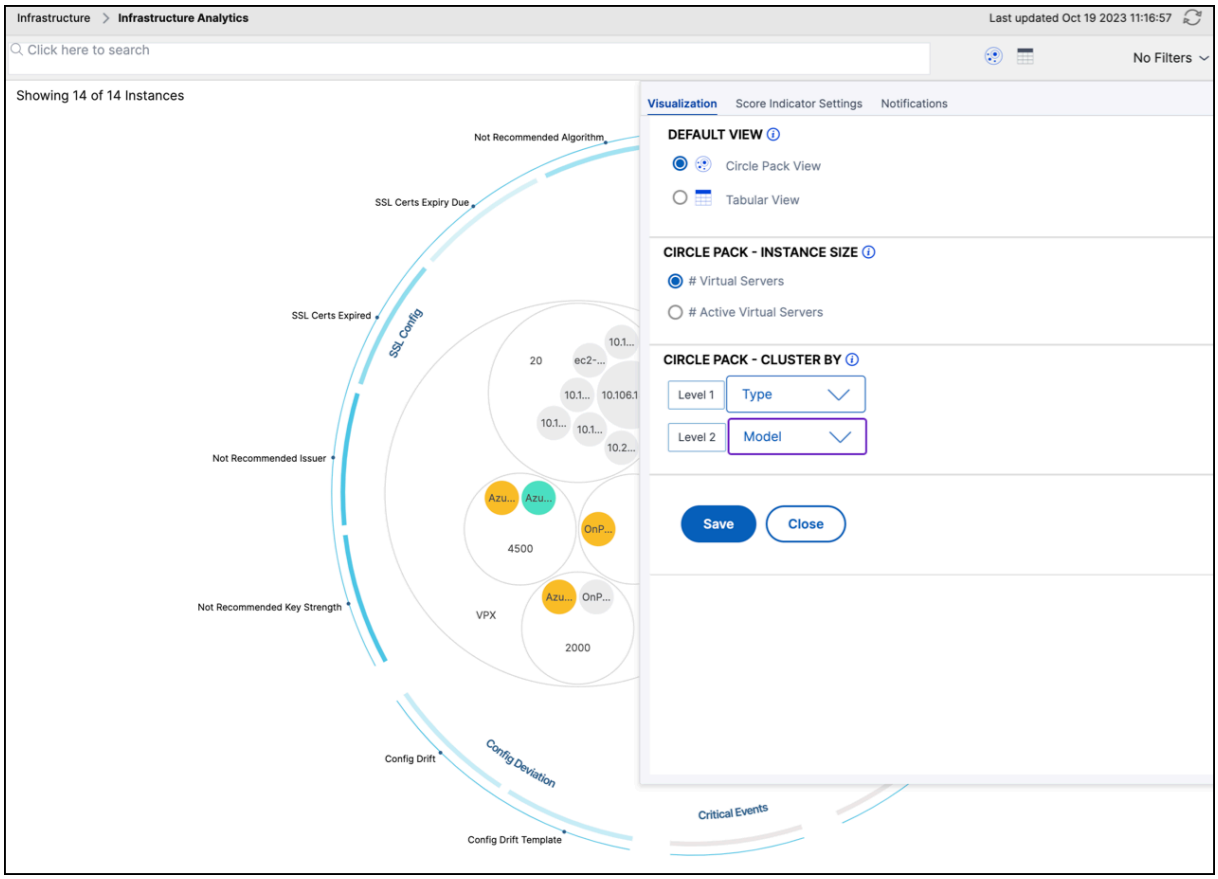
所有这些嵌套圆圈都由两个最外面的圆圈界限。外面的两个圆圈代表 NetScaler 控制台监视的四类事件（系统资源、关键事件、SSL 配置和配置偏差）以及相关的运行状况指标。

群集实例圈

NetScaler 控制台监视许多实例。为了简化对这些实例的监视和维护，基础设施分析允许您将它们分为两个级别。也就是说，实例分组可以嵌套在另一个分组中。

例如，BLR 数据中心有两种类型的 NetScaler 实例——VPX 和 MPX，部署在其中。您可以先按类型对 NetScaler 实例进行分组，然后按对它们进行分组的站点对所有实例进行分组。现在，您可以轻松识别在您管理的站点中部署了多少类型的实例。

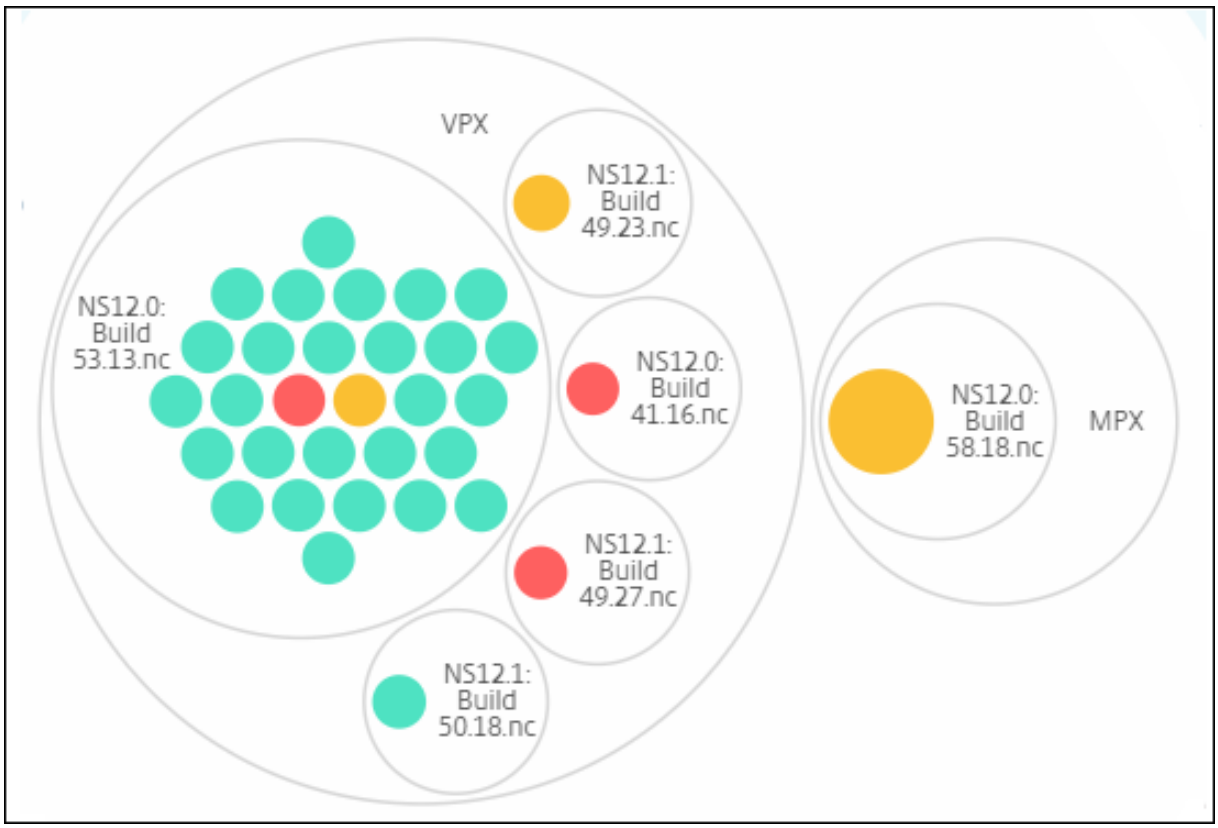




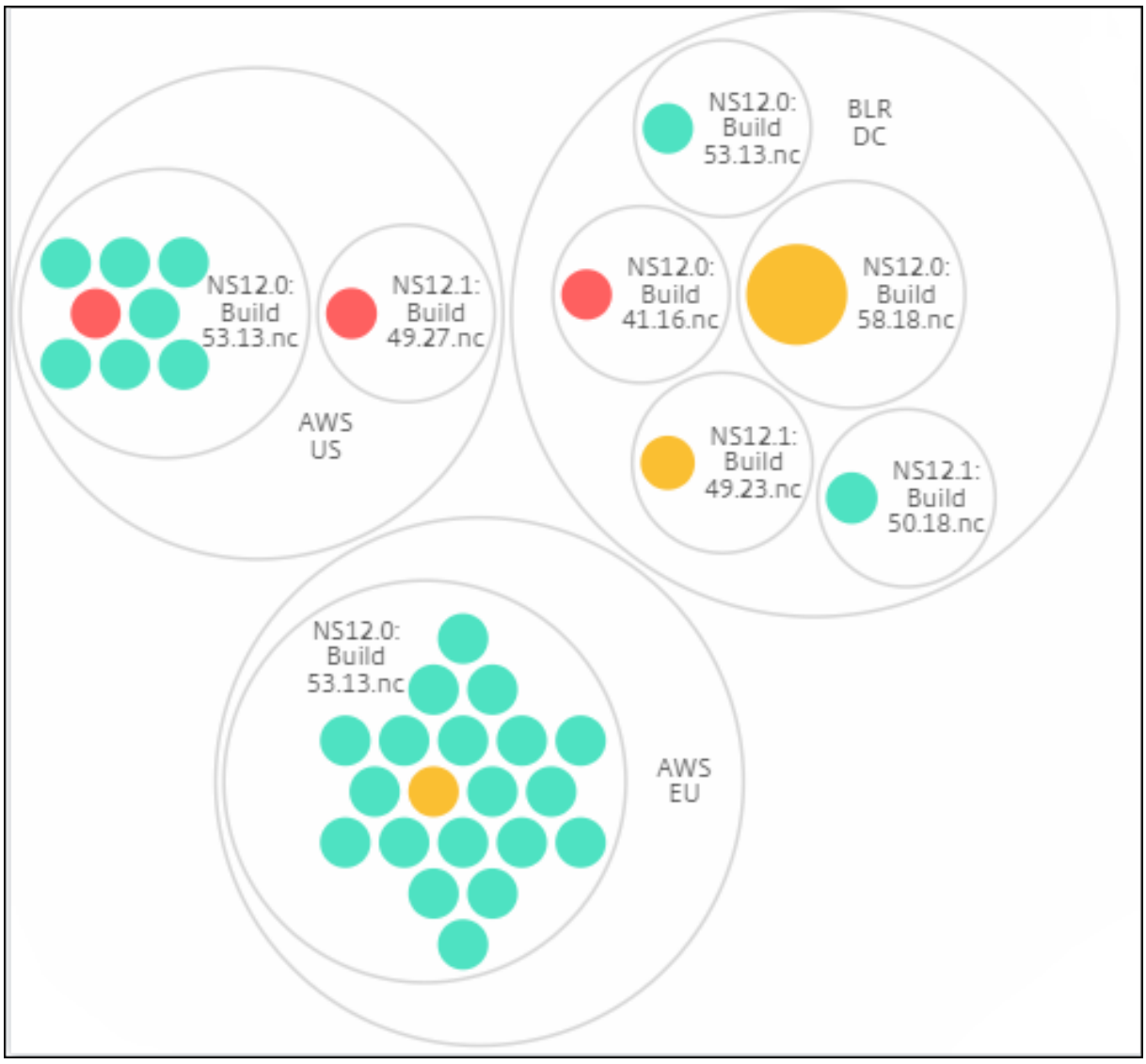
两级聚类的其他几个示例如下：

地点和型号：

类型和版本：

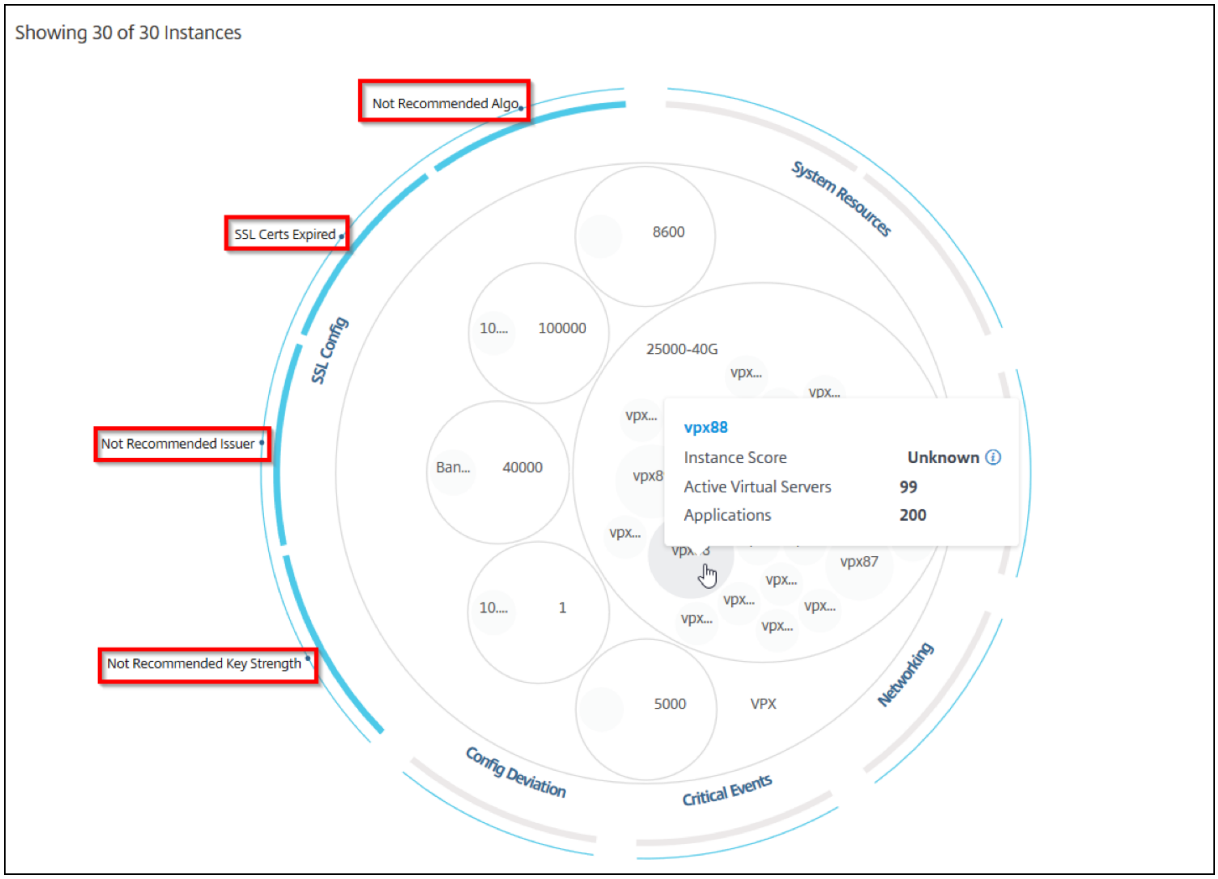


站点和版本：



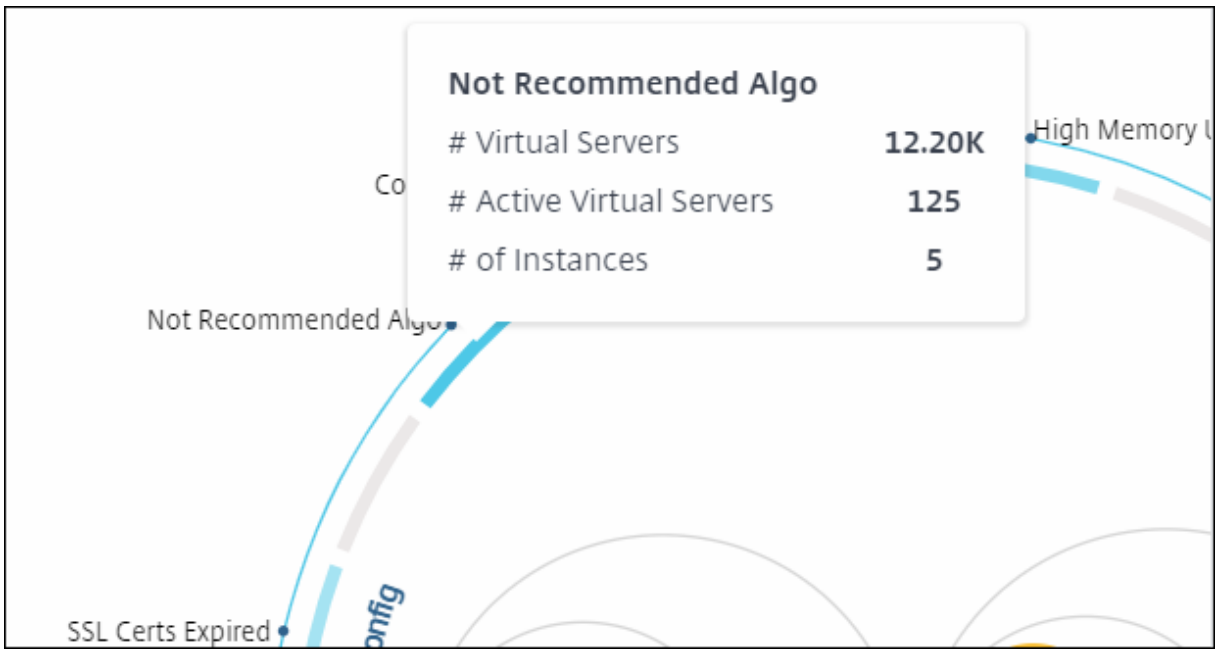
如何使用 **Circle Pack**

单击每个彩色圆圈以突出显示该实例。



根据在这种情况下发生的事件，只有这些运行状况指标在外圈突出显示。例如，以下两个 Circle Pack 图像显示不同的风险指标集，尽管这两个实例都处于严重状态。

您还可以单击运行状况指标以获取有关报告该风险指标的实例数量的更多详细信息。例如，单击 `Not recommended Algo` 查看该风险指标的摘要报告。



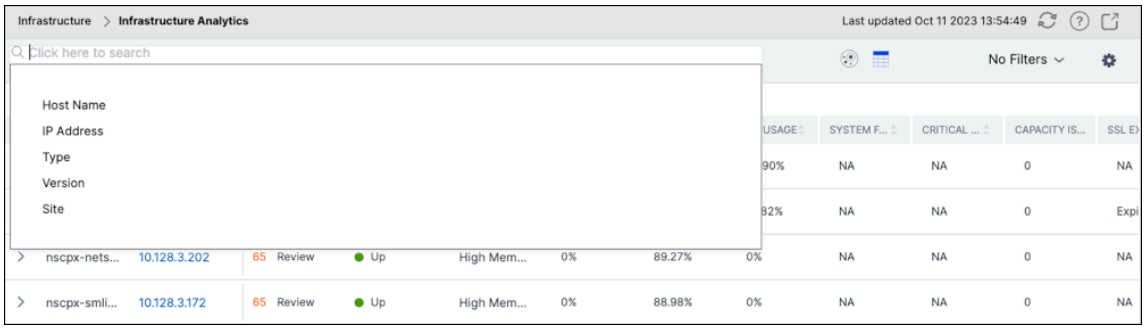
表格视图

表格视图以表格格式显示实例和这些实例的详细信息。有关更多信息，请参阅 实例详情

搜索栏

将鼠标光标置于搜索栏上，然后选择以下搜索属性以筛选结果：

- 主机名
- IP 地址
- 类型
- 版本
- 站点



搜索结果适用于圆视图和表格视图。

如何使用摘要面板

摘要面板 可帮助您高效、快速地专注于需要审核或关键状态的实例。该面板分为三个选项卡-概述、实例信息和流量概况。您在此面板中所做的更改会修改圆形包和表格视图格式的显示。以下各节更详细地描述了这些选项卡。以下部分中的示例可帮助您有效地使用不同的选择标准来分析实例报告的问题。

概述：

概述 选项卡允许您根据硬件错误、使用情况、过期证书和实例中可能出现的类似指标来监视实例。您可以在此处监视的指标如下：

- CPU 使用率
- 内存使用率
- 磁盘使用情况
- 系统故障
- 关键事件
- SSL 证书到期

有关这些指标的更多信息，请参阅 *NetScaler* 实例中的运行状况指标。

以下示例说明了如何与概述面板交互以隔离那些报告错误的实例。

示例 **1**：查看处于审阅状态的实例：

选中“查 看”复选框以仅查看那些未报告严重错误但仍需要注意的实例。

概述 面板中的直方图表示基于高 CPU 使用率、高内存使用率和高磁盘使用率事件的实例聚合数。直方图的分级分别为 10%、20%、30%、40%、50%、60%、70%、80%、90% 和 100%。将鼠标指针悬停在其中一个条形图上。图表底部的图例显示使用范围和该范围内的实例数。您也可以单击条形图以显示该范围内的所有实例。

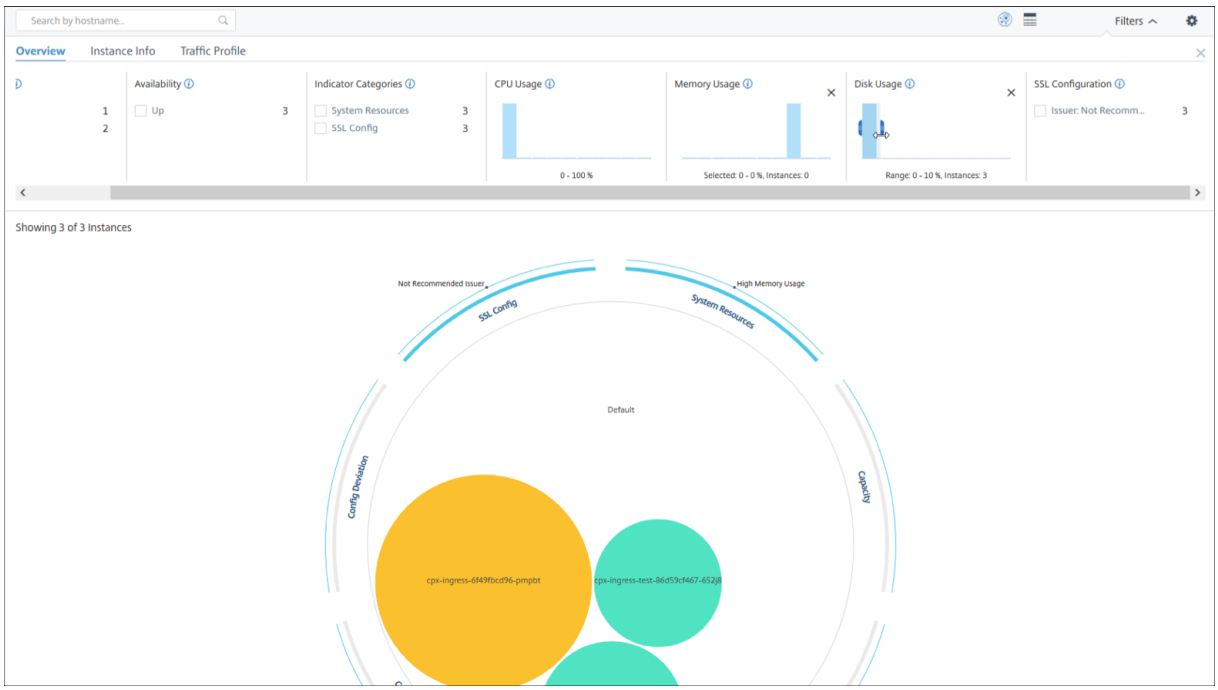
示例 **2**：查看消耗分配内存的 **10%** 到 **20%** 的实例：

在内存使用情况部分中，单击条形图。图例显示所选范围为 10-20%，该范围内有 29 个实例在运行。

您也可以在这些直方图中选择多个范围。

示例 **3**：查看在多个范围内消耗磁盘空间的实例：

要查看消耗内存在 0% 到 10% 磁盘空间之间的实例，请将鼠标指针拖到两个范围上，如下图所示。



> 注意：
>
> 单击“X”移除选择。您也可以单击“重置”以删除多个选择。

概述 面板中的水平条形图表示报告系统错误、严重事件和 SSL 证书到期状态的实例数量。选中该复选框可查看这些实例。

示例 **4**：查看过期 **SSL** 证书的实例：

在 **SSL** 证书到期 部分中，选中“已过期”复选框以查看这三个实例。

1 -单击 筛选器 列表。

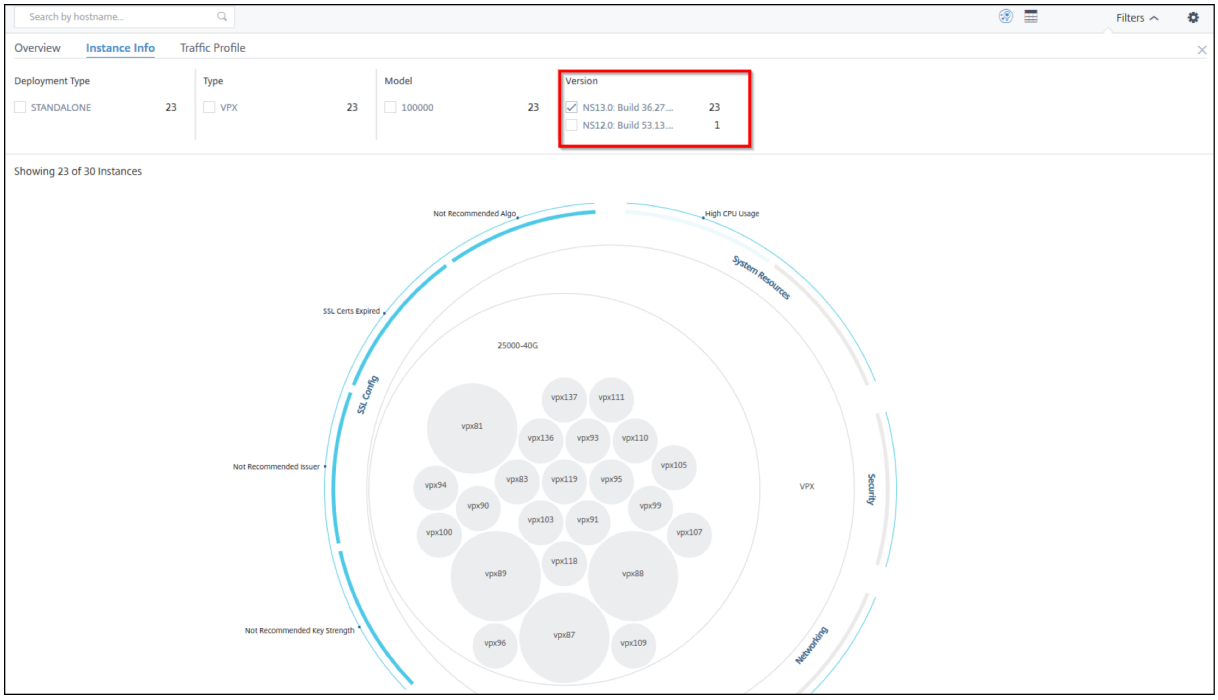
2 -在 **SSL** 证书到期 部分，选中“已过期”复选框以查看实例。

实例信息

实例信息 面板允许您根据部署类型、实例类型、模型和软件版本查看实例。您可以选中多个复选框来缩小选择范围。

示例 **5**：查看具有特定内部版本号的 **NetScaler VPX** 实例：

选择要查看的版本。

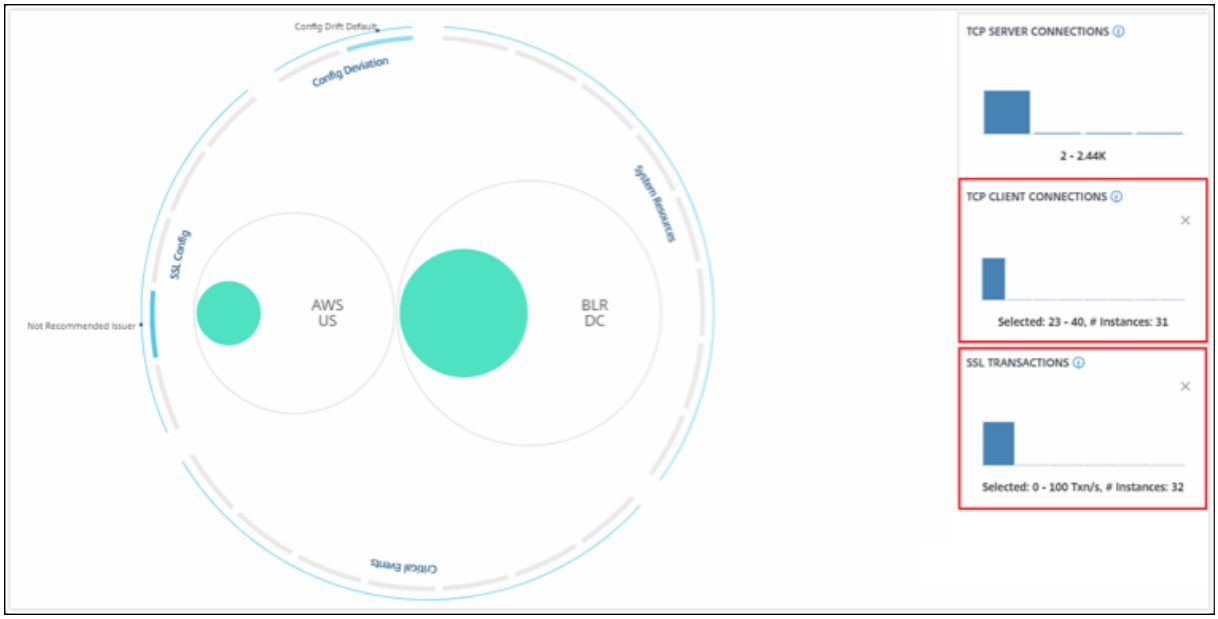


流量配置文件

Traffic p **ro** file 面板中的直方图表示基于实例的许可吞吐量、请求数量、连接数和实例处理的事务的实例聚合数。选择条形图以查看该范围内的实例。

示例 **6**：查看支持 **TCP** 连接的实例：

下图显示了支持 23 到 40 之间的 TCP 连接以及每秒最多处理 100 个 SSL 事务的实例数量。



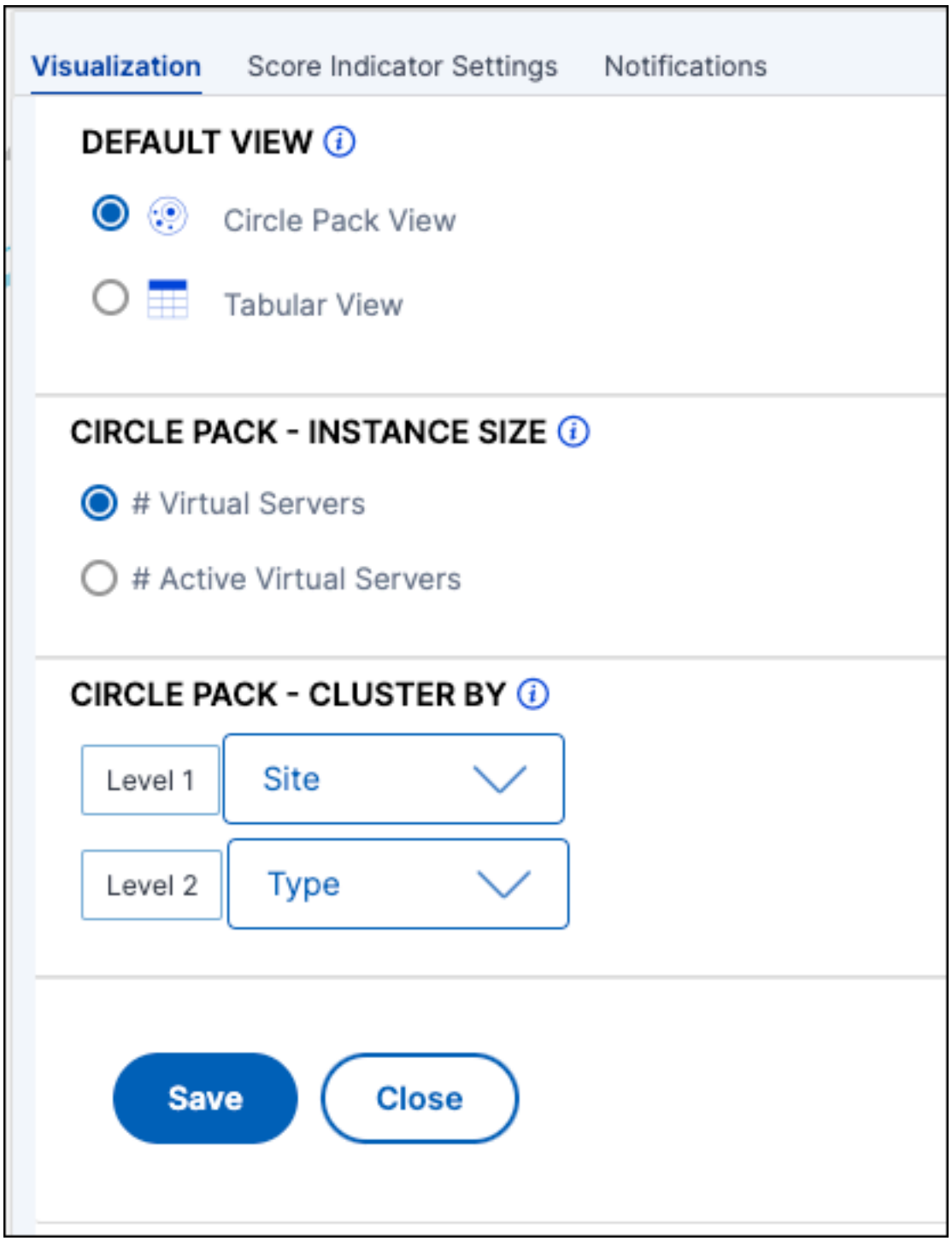
如何使用设置面板

设置 面板允许您：

- 设置基础设施分析的默认视图。
- 为高 CPU 使用率、高磁盘使用率和高内存使用率设置低阈值和高阈值。
- 选择实例指标，配置阈值并为这些指标分配权重以计算实例得分
- 选择所需的问题，针对超过配置阈值的问题启用通知，并仅接收选定问题的通知。

查看

- 默认视图。选择 圆形包 或表格格式作为分析页面上的默认视图。您选择的格式就是您在 NetScaler 控制台中访问该页面时所看到的格式。
- 圆形包装**-**实例大小。允许实例圈的大小乘以虚拟服务器的数量或活动虚拟服务器的数量。
- **Circle Pack-**聚类依据。确定实例圆的两级聚类。有关实例群集的更多信息，请参阅 群集实例圈。



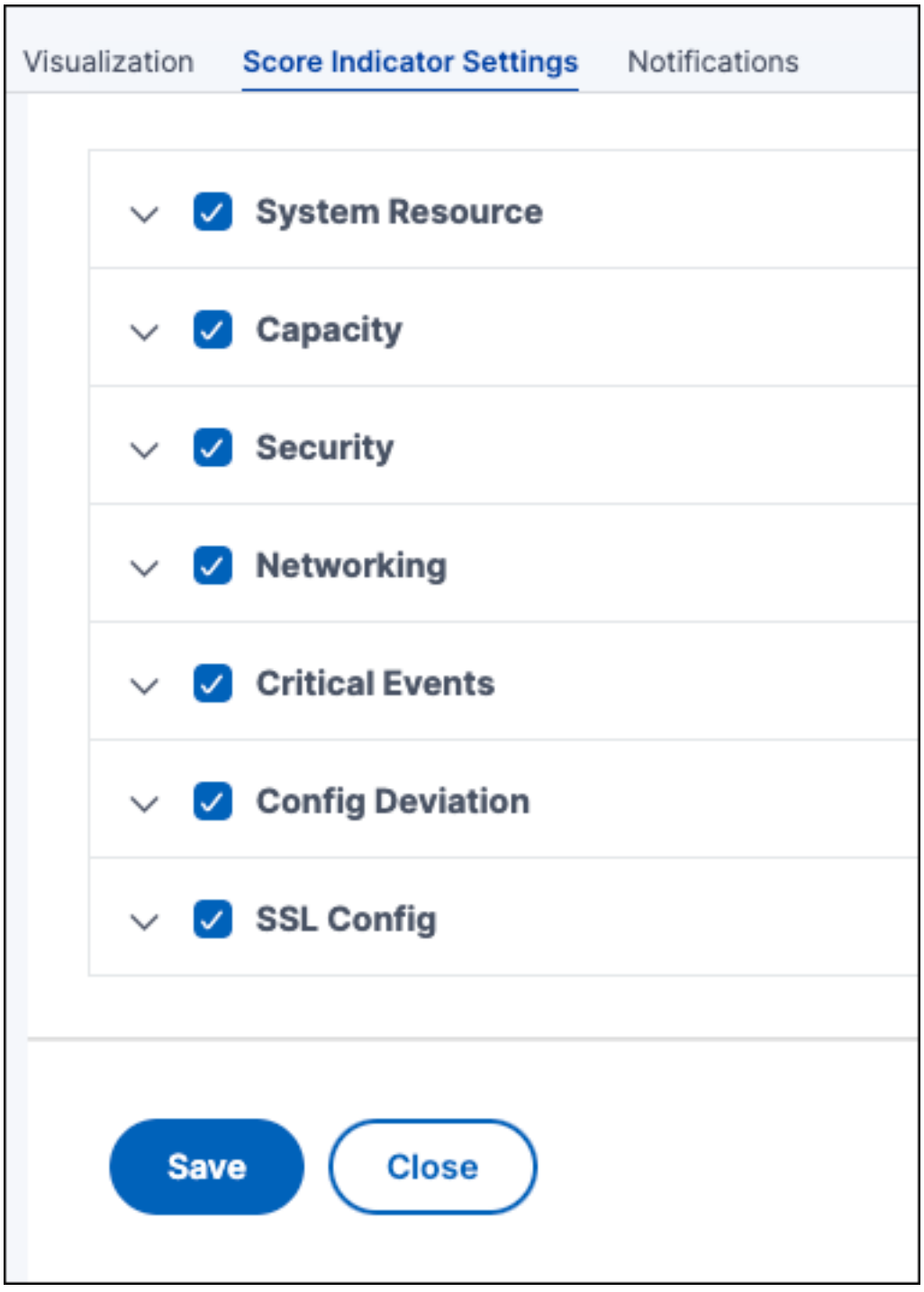
选择指标并自定义权重以进行例如得分计算

您可以选择实例指标、配置阈值并为这些指标分配权重以计算实例得分。默认情况下，选择所有指标，并为每个指标分配默认权重。您可以根据自己的要求选择指标并分配合适的权重来确定实例得分的计算。

单击“设置”图标并选择“得分指示器设置”选项卡以：

- 选择所需的指标并添加阈值
- 为指标分配权重。

配置阈值并分配权重后，单击“保存”。实例得分仅根据所选指标及其权重进行更新。

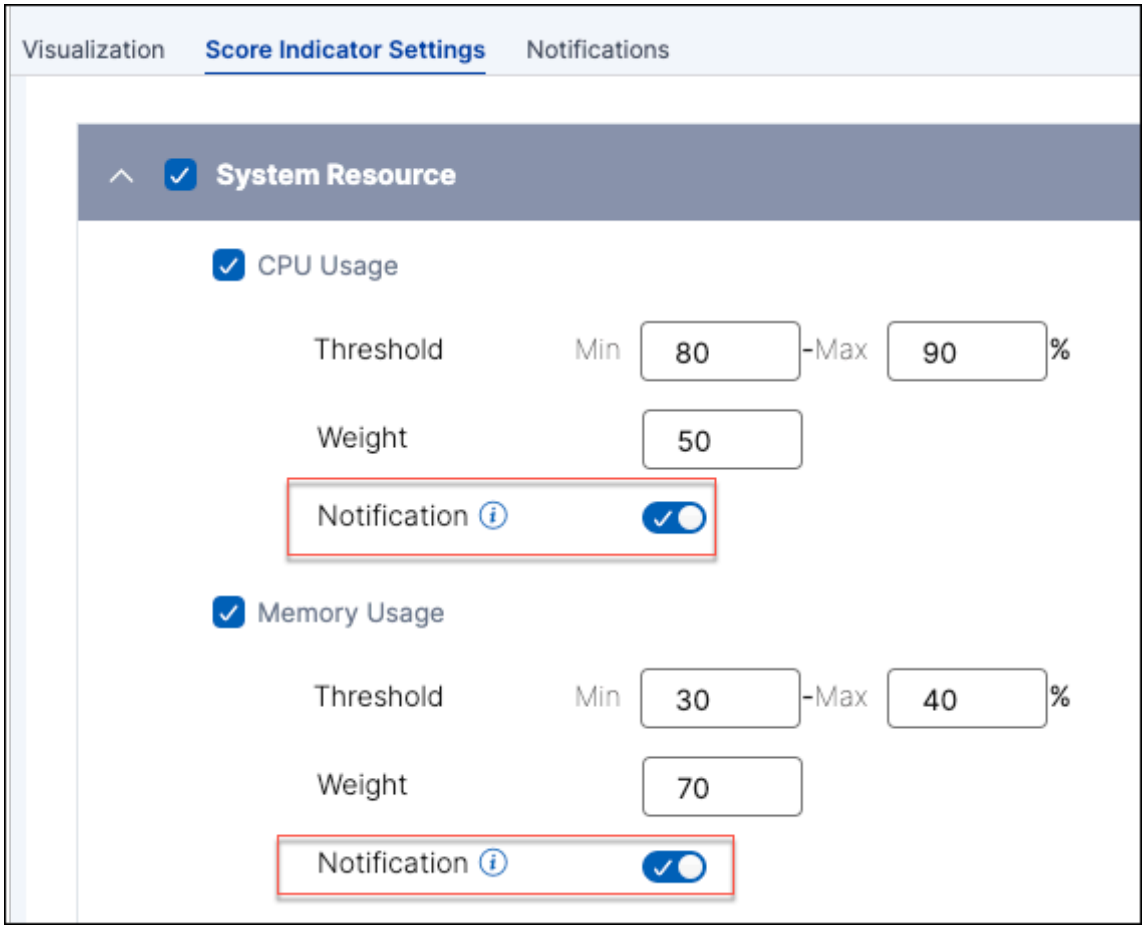


配置通知

您可以选择所需的问题，为超过配置阈值的问题启用通知，并仅接收选定问题的通知。此增强功能使您能够仅接收有关要监视的选定问题的通知。

> 注意：
>
> 默认情况下，会选择所有类别下的议题。您只能为可以配置阈值的问题启用通知。

1. 单击“设置”图标并选择“得分指示器设置”选项卡。
2. 选择您想要接收通知的问题。
3. 对于“系统资源”和“容量”类别下的问题，启用 通知。



4. 单击保存。

> 注意：
>
> 必须确保在“通知”选项卡中配置至少一个配置文件。

如何在控制板上可视化数据

使用基础结构分析，网络管理员现在可以在几秒钟内识别需要最多关注的实例。为了更详细地了解这一点，让我们来看看 ExampleCompany 的网络管理员 Chris 的案例。

克里斯在他的组织中维护着许多 NetScaler 实例。一些实例处理高流量，他需要密切监视它们。他注意到一些高流量实例不再处理通过它们的全部流量。为了分析这种减少，早些时候，他不得不阅读来自不同来源的多份数据报告。Chris 不得不花更多的时间尝试手动关联数据，找出哪些实例未处于最佳状态，需要注意。他使用基础设施分析功能直观地查看所有实例的运行状况。

以下两个示例说明了基础结构分析如何帮助 Chris 进行维护活动：

示例 **1-**监视 **SSL** 流量：

Chris 在 Circle Pack 上注意到，一个实例的实例得分较低，并且该实例处于“严重”状态。他点击实例看看问题出在哪里。实例摘要显示该实例上存在 SSL 卡故障，因此该实例无法处理 SSL 流量（SSL 流量已减少）。Chris 提取这些信息，并向团队发送一份报告，以便立即调查问题。

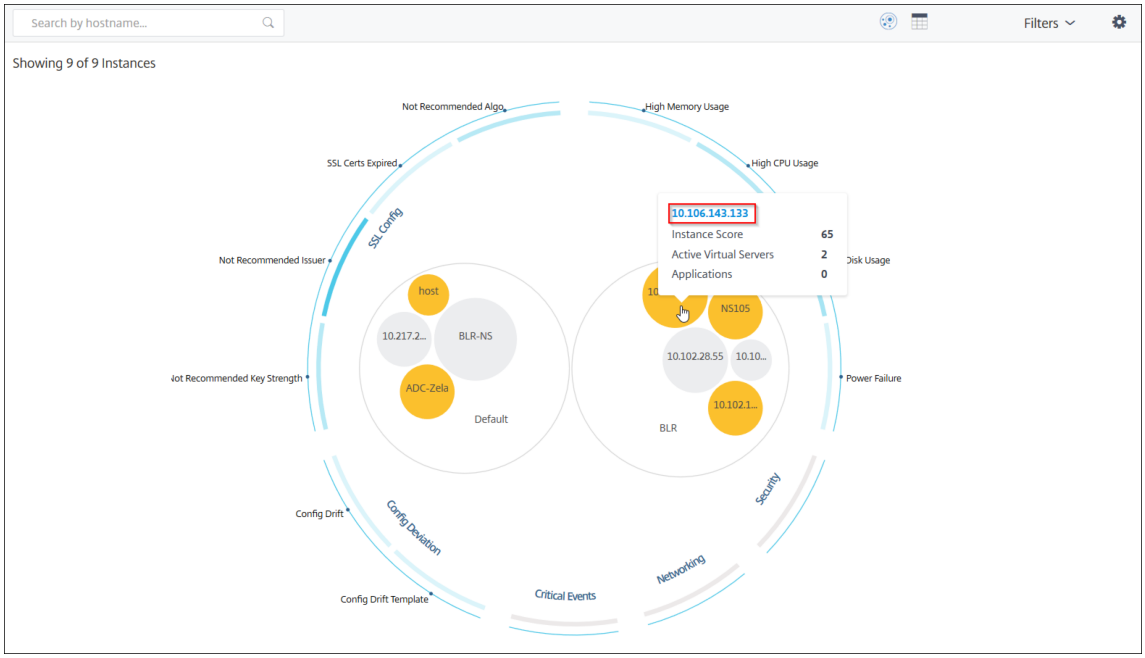
示例 **2-**监视配置更改：

Chris 还注意到另一个实例处于“审查”状态，并且最近出现了配置偏差。当他点击配置偏差风险指示器时，他注意到已经进行了与 RC4 Cipher、SSL v3、TLS 1.0 和 TLS 1.1 相关的配置更改，这可能是出于安全考虑。他还注意到此实例的 SSL 事务流量配置文件已关闭。他导出此报告并将其发送给管理员进一步查询。

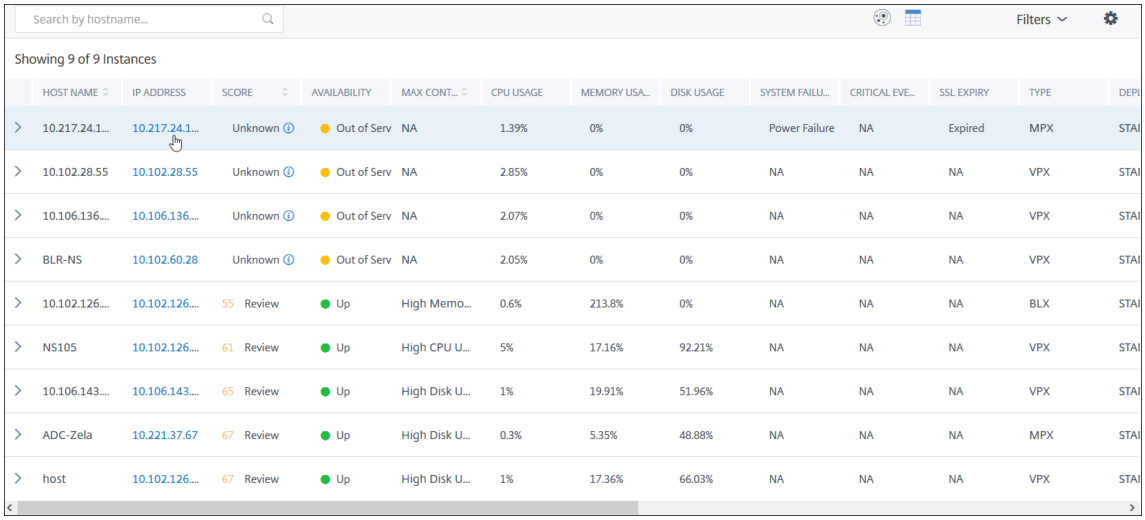
在基础结构分析中查看实例详细信息

January 29, 2024

1. 导航到 基础结构 **>** 基础结构分析。
2. 单击圆包视图并选择 IP 地址。



您也可以单击表格视图中的 IP 地址。



- 主机名—表示分配给 NetScaler 实例的主机名
- **IP** 地址—表示 NetScaler 实例的 IP 地址
- 评分—表示 NetScaler 实例评分和“关键”、“良好”和“一般”等状态
- 可用性—表示 NetScaler 实例的当前状态，例如 启动、关闭或停止服务。
- 最大贡献—表示 NetScaler 实例具有最大错误数的问题类别。
- **CPU** 使用率—表示实例当前使用的 CPU 百分比
- 内存使用率—表示实例当前使用的内存百分比
- 磁盘使用率—表示实例当前使用的磁盘百分比

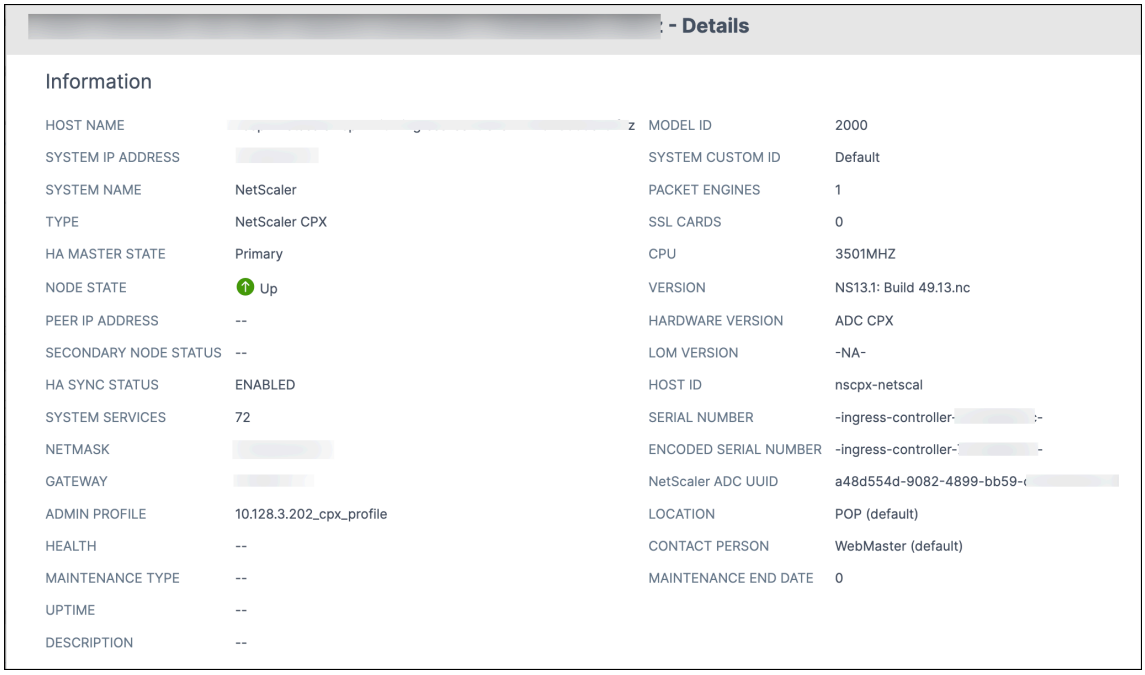
- 系统故障—表示实例系统的错误总数
- 严重事件—表示 NetScaler 实例具有最大事件的事件类别
- **SSL** 到期—表示安装在 NetScaler 实例上的 SSL 证书的当前状态
- 类型—表示 NetScaler 实例类型，例如 VPX、SDX、MPX 或 CPX
- 部署—表示 NetScaler 实例是作为独立实例还是 HA 对进行部署
- 型号—表示 NetScaler 实例型号
- 版本—表示 NetScaler 实例版本和内部版本号
- 吞吐量—表示来自 NetScaler 实例的当前网络吞吐量
- **HTTPS** 请求/秒—表示 NetScaler 实例收到的当前 HTTPS 请求/秒
- **TCP** 连接 -表示当前建立的 TCP 连接
- **SSL** 交易—表示 NetScaler 实例处理的当前 SSL 交易
- 站点—表示部署 NetScaler 实例的站点名称。

> 注意：
>
> 每 5 分钟更新一次 CPU 使用率、内存使用率、磁盘使用率、吞吐量等的当前值。

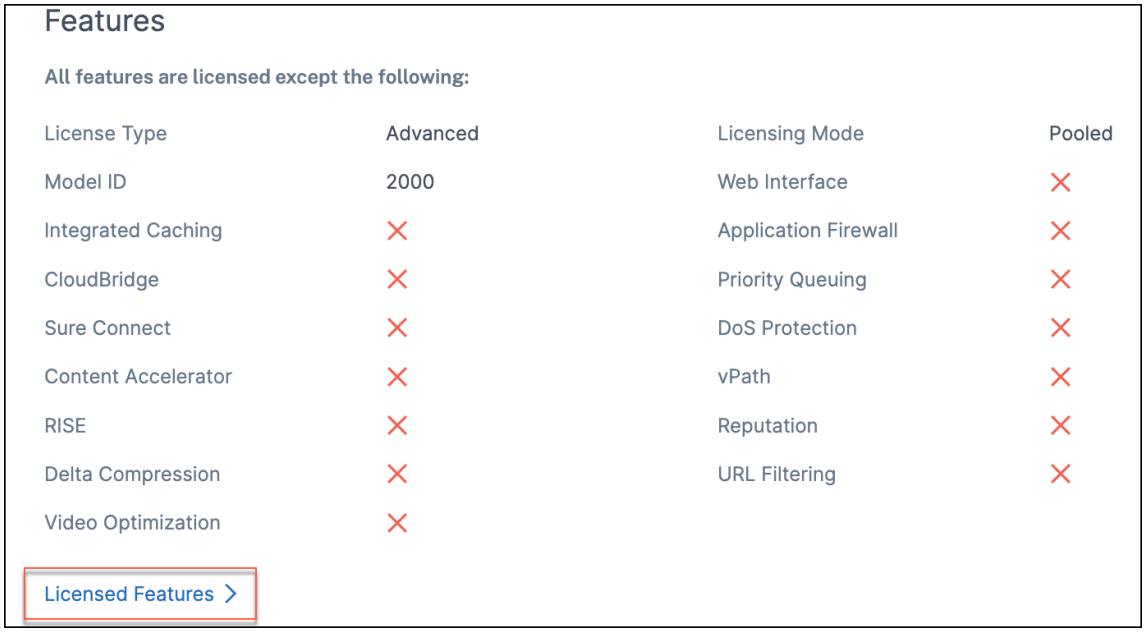
单击 IP 地址，然后在出现的页面中，单击“实例详细信息”以查看实例详细信息。

将显示以下详细信息：

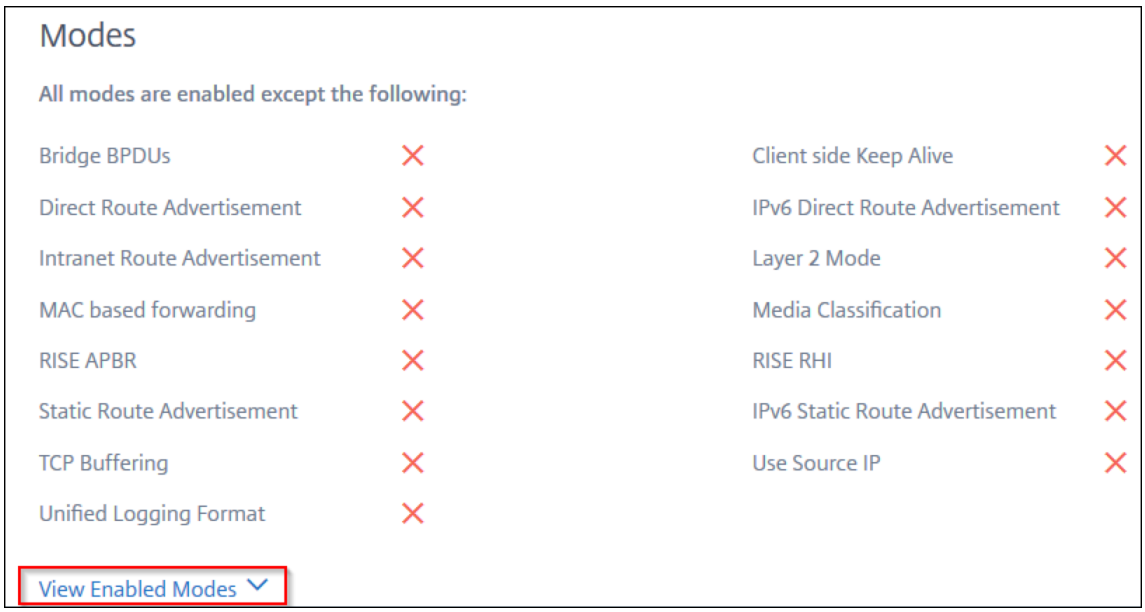
- 信息 -实例详细信息，例如实例类型、部署类型、版本、型号等。



- 功能 -默认情况下，显示未获得许可的功能。单击“许可功能”查看已许可的功能。

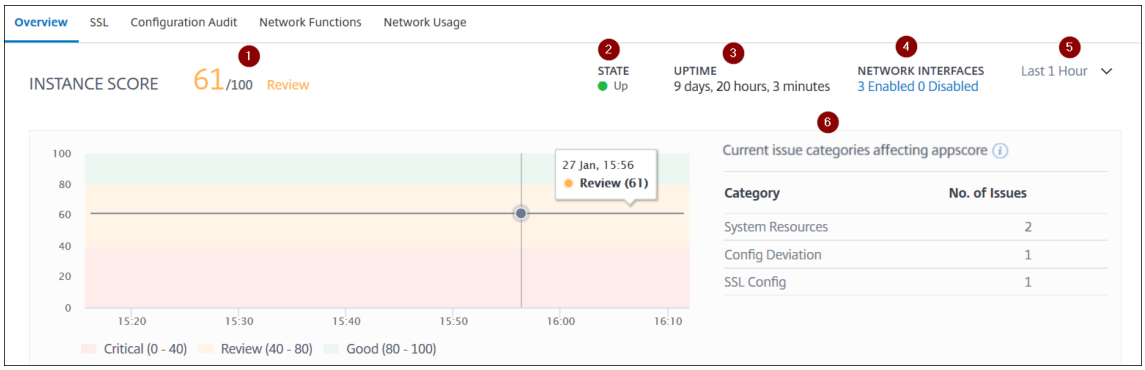


- 模式 -默认情况下，显示在实例上禁用的所有模式。单击“查看启用模式”以查看实例上的启用模式。



实例控制板显示实例概述，您可以在其中查看以下详细信息：

- 实例得分



1 —表示选定持续时间内的当前 NetScaler 实例得分。最终得分以 **100** 减去总点球计算。图形显示选定时间持续时间的得分范围。

2 —表示 NetScaler 实例的当前状态，例如启动、关闭和不服务。

3 —表示 NetScaler 实例启动并运行的持续时间。

4 —表示实例启用和禁用的网络接口总数。单击“启用”或“已 禁用”可查看网络接口名称和状态（启用或禁用）等详细信息。

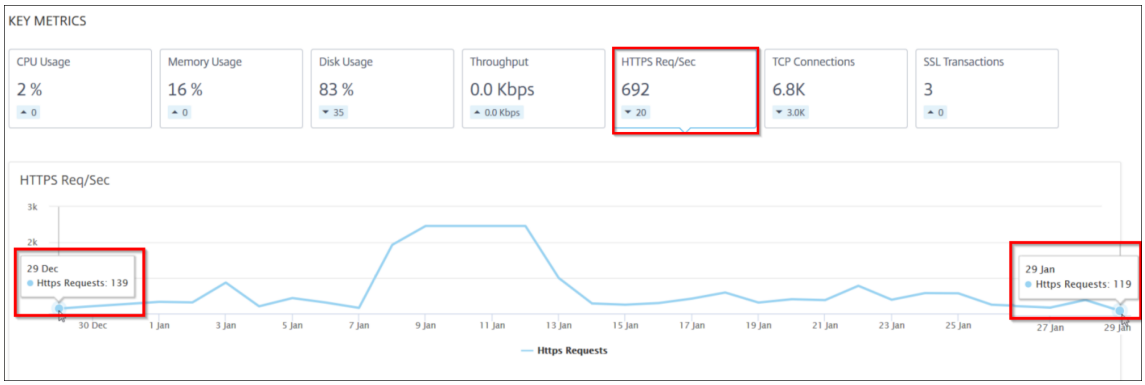
5 —从列表中选择持续时间以查看实例详细信息。

6—显示 NetScaler 实例的总问题和问题类别。

- 关键指标

  单击每个选项卡查看详细信息。在每个指标中，您可以查看所选时间的平均值和差值。

下图是 HTTPS Req/Sec 的示例，所选持续时间为 1 小时。值 **692** 是 1 个月持续时间内的平均 HTTPS 请求/秒，值 **20** 是差值。在图形中，第一个值为 **139** ，最后一个值为 **119**。差值为 **139 —119 = 20**。



您可以在所选时间持续时间内以图形格式查看以下实例指标：

- **CPU** 使用率 -选定持续时间内实例的平均 CPU 百分比（显示数据包 CPU 和管理 CPU）。
- 内存使用率—选定持续时间内实例的平均内存使用百分比。
- 磁盘使用率—选定持续时间内实例的平均磁盘空间百分比。
- 吞吐量—实例在选定持续时间内处理的平均网络吞吐量。
- **HTTPS** 请求/秒—实例在所选时长内收到的平均 HTTPS 请求数。
- **TCP** 连接 -客户端和服务器在选定持续时间内建立的平均 TCP 连接。
- **SSL** 事务—实例在选定持续时间内处理的平均 SSL 事务。

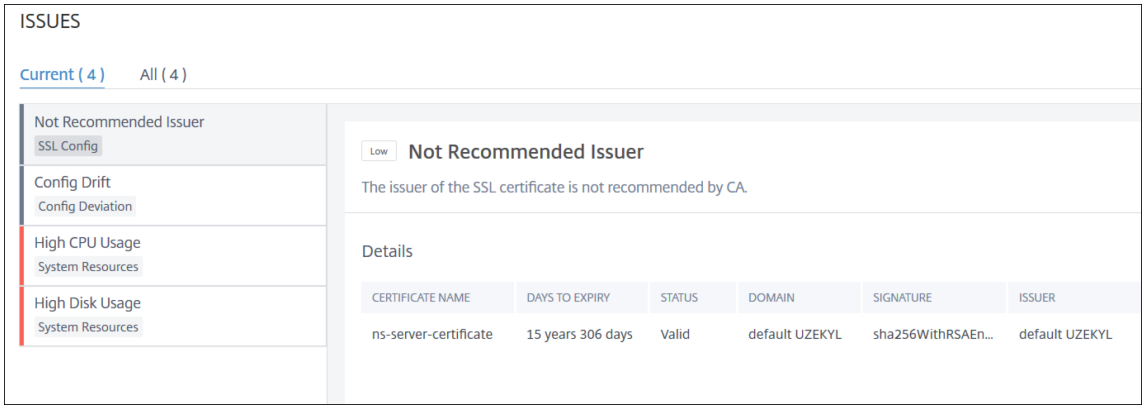
- 问题

  您可以查看 NetScaler 实例中出现的以下问题：

问题类别	说明	问题
系统资源	显示与 NetScaler 系统资源相关的所有问题，例如 CPU、内存、磁盘使用情况等。	– 高 CPU 使用率 – 高内存使用率 – 高磁盘使用率 – SSL 卡故障 – 电源故障 – 磁盘错误 – 闪存错误 – 网卡丢弃

问题类别	说明	问题
SSL 配置	显示与 NetScaler 实例上的 SSL 配置相关的所有问题。	-SSL 证书已过期 – 不建议发行人 – 不建议 Algo – 不建议密钥强度
配置偏差	显示与 NetScaler 实例中应用的配置作业相关的所有问题。	-配置偏移 – 运行与模板
关键事件	显示与在 HA 对和群集中配置的 NetScaler 实例相关的所有关键事件。	– 群集道具故障 – 群集同步失败 – 群集版本不匹配 – HA 次要状态不正确 – HA 无热节拍 – HA 同步失败 – HA 版本不匹配
容量问题	显示 NetScaler 容量问题。NetScaler 控制台每五分钟从 NetScaler 实例轮询这些事件，并显示丢包情况或速率限制计数器增量（如果存在）。这些问题根据以下容量参数进行分类。	– 已达到吞吐量限制
网络连接	显示实例中出现的操作问题。	有关更多信息，请参阅 使用新指标增强的基础设施分析。

单击每个选项卡以分析问题并进行故障排除。例如，假设一个实例在选定的持续时间内存在以下错误：



- “当前”选项卡显示当前影响实例得分的问题。
- “全部”选项卡显示在选定持续时间内检测到的所有问题。

查看 **NetScaler** 实例中的容量问题

January 29, 2024

当 NetScaler 实例消耗了其大部分可用容量时，在处理客户端流量时可能会丢包。此问题会导致 NetScaler 实例性能低下。通过了解此类的 NetScaler 容量问题，您可以主动分配额外的许可来稳定 NetScaler 性能。

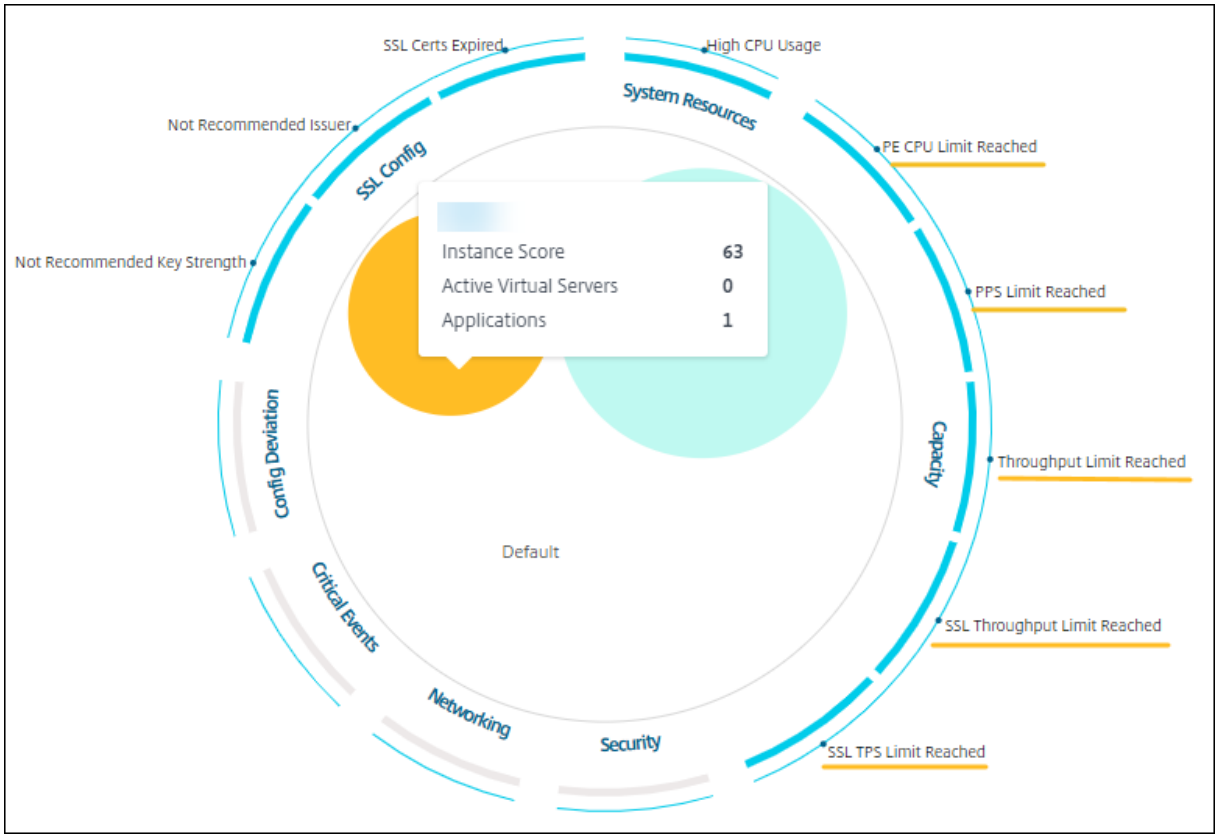
在 **Circle Pack View** 中，您可以查看 NetScaler 实例容量问题（如果存在）。

要查看 NetScaler 容量问题，

1. 导航到 基础结构 **>** 基础结构分析。
2. 选择圆包视图。

> 注意：
>
> 在 基础设施分析中，圆形视图和表格视图显示了过去一小时内发生的事件和问题。

下图表明选定实例中存在容量问题：



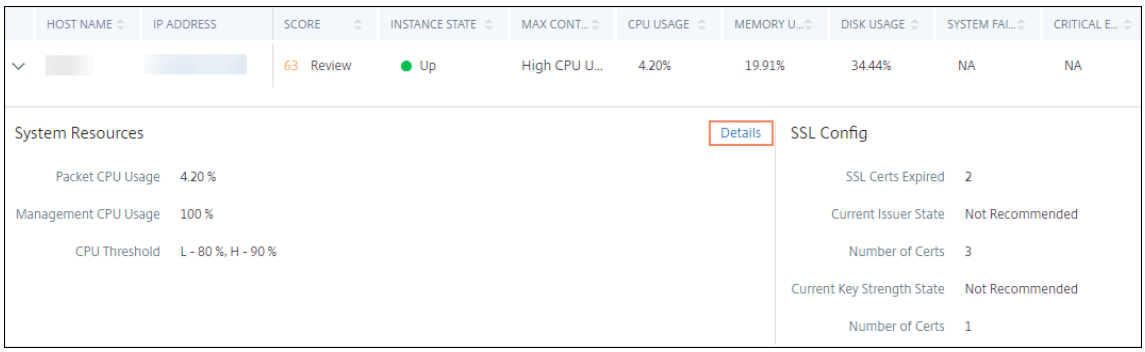
这些问题按以下容量参数分类：

- 达到吞吐量限制-达到 吞吐量限制后实例中丢弃的数据包数量。
- 已达到 **PE CPU** 限制-达到 PE CPU 限制后在所有 NIC 上丢弃的数据包数量。
- 已达到 **PPS** 限制-达到 PPS 限制后实例中丢弃的数据包数量。
- **SSL** 吞吐量速率限制 -达到 SSL 吞吐量限制的次数。
- **SSL TPS** 速率限制—达到 SSL TPS 限制的次数。

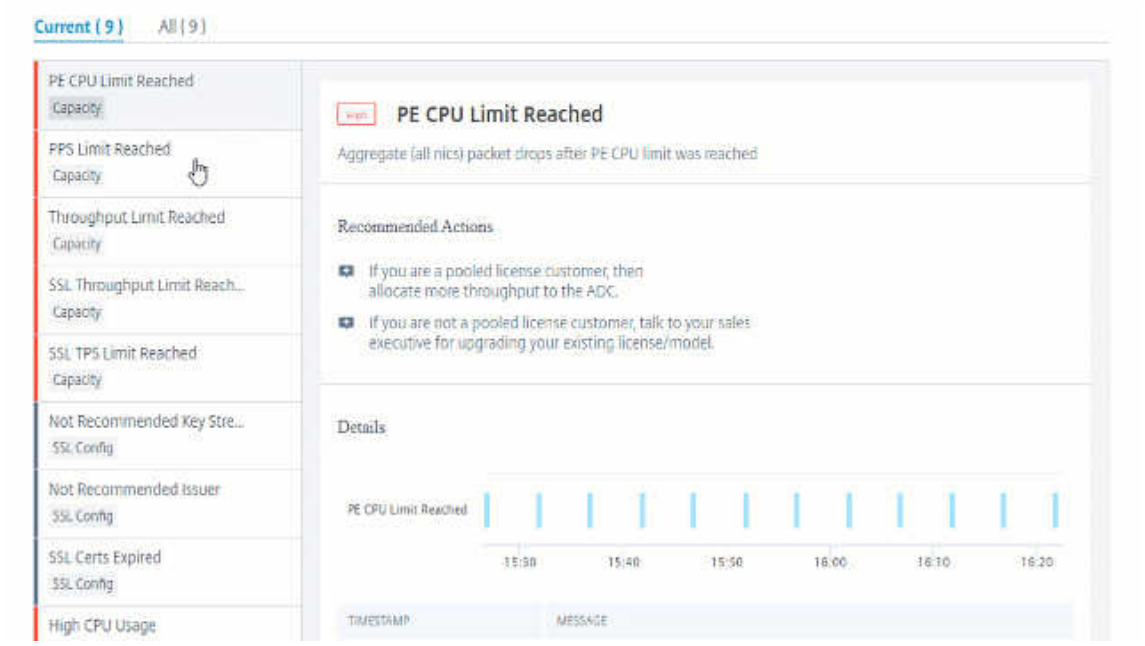
查看解决容量问题的建议措施

NetScaler 控制台推荐可以解决容量问题的操作。要查看建议的操作，请执行以下步骤：

1. 在 基础结构 **>** 基础结构分析中，选择表格视图。
2. 选择存在容量问题的实例，然后单击 详细信息。



3. 在实例页面中，向下滚动到 问题 部分。
4. 选择每个问题并查看解决容量问题的建议措施。



NetScaler 控制台每五分钟从 NetScaler 实例轮询这些事件，并显示丢包情况或速率限制计数器增量（如果存在）。

NetScaler 控制台根据定义的容量阈值计算实例评分。

- 低阈值—1 个数据包丢弃或速率限制计数器增量
- 高阈值—10000 个数据包丢弃或速率限制计数器增量

因此，当 NetScaler 实例突破容量阈值时，实例评分会受到影响。

当数据包丢弃或速率限制计数器递增时，将在 ADCCapacityBreach 类别下生成一个事件。要查看这些事件，请导航到“设置” > “系统事件”。

利用新指标增强的基础结构分析

January 29, 2024

使用 NetScaler 控制台基础架构分析，您可以：

- 查看 NetScaler 实例中出现的一系列新的操作问题。
- 查看错误消息并查看建议以解决问题。

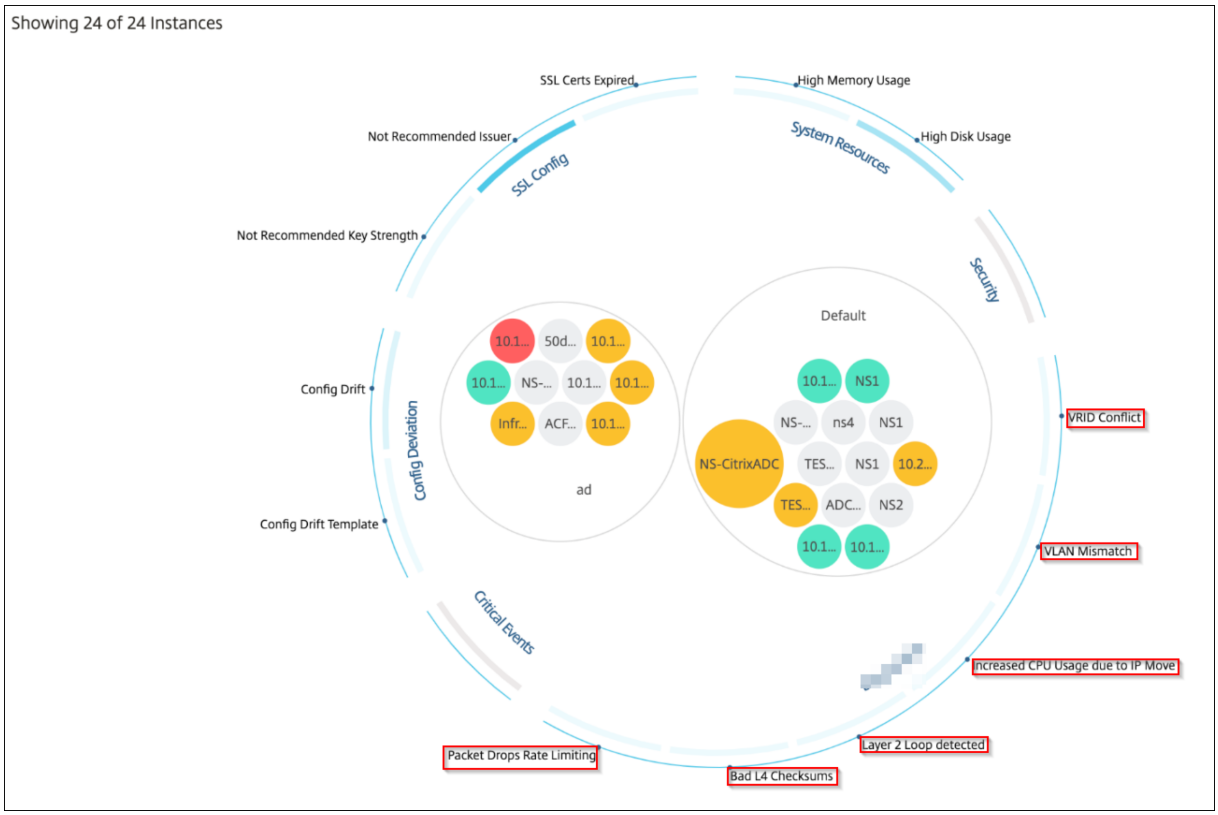
作为管理员，您可以快速确定问题的根本原因分析。

> 注意：
>
> 规则指示器不支持以下用途：
>
> - 在群集模式下配置的 NetScaler 实例。
> - 配置了管理分区的 NetScaler 实例。

在 NetScaler 控制台中，导航 到基础架构 **>** 基础 架构分析，查看以下指标：

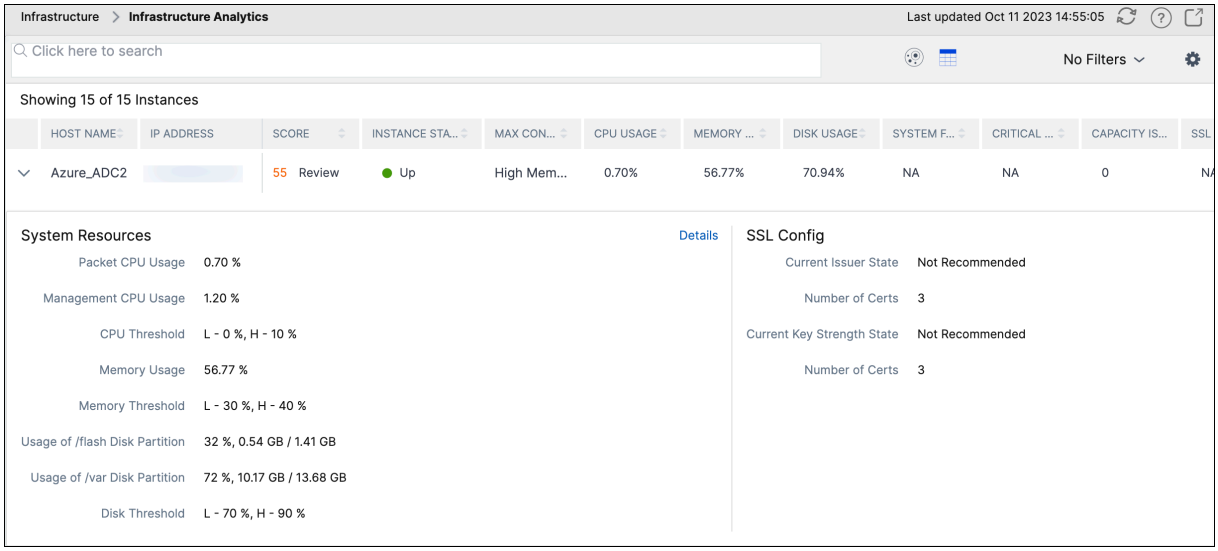
基础结构分析中的指标名称	说明
端口分配失败	检测 NetScaler 何时使用 SNIP 与新的服务器连接进行通信，并且该 SNIP 上的可用端口总数已耗尽。建议采取的操作是在同一子网中添加另一个 SNIP。
会话累积	检测 NetScaler 内存何时被 SSL 会话占用。
无默认路由配置	检测何时由于路由不可用而导致流量丢失。
IP 冲突	检测是否在网络中的两个或多个实例上配置或应用了相同的 IP 地址。
VRID 冲突	检测指定 VRID 何时出现间歇性访问问题。
VLAN 不匹配	检测在绑定到 IP 子网的 VLAN 配置期间是否出现任何错误。
TCP 小窗口攻击	检测何时可能存在小窗口攻击。此警报仅供参考，因为 NetScaler 已经缓解了这种攻击。
速率控制阈值	根据配置的速率控制阈值检测数据包何时被丢弃。
持久性限制	检测何时对 NetScaler 内存施加最大命中率。
GSLB 站点名称不匹配	检测何时由于站点名称不匹配而发生 GSLB 配置同步故障。
IP 标头格式不正确	检测 IPv4 数据包的健全性检查何时失败。
错误的 **L4** 校验和	检测 TCP 数据包的校验和验证何时失败。

基础结构分析中的指标名称	说明
由于 **IP** 移动而增加 **CPU** 使用率	检测是否需要更新大量 Mac。
数据包转向过多	检测由于使用非对称 rss 密钥类型而导致的高水平软件数据包转向。
第 **2** 层环路	检测网络中是否存在第 2 层环路。
标记 **VLAN** 不匹配	检测何时在无标记接口上接收到带标记的 VLAN 数据包。



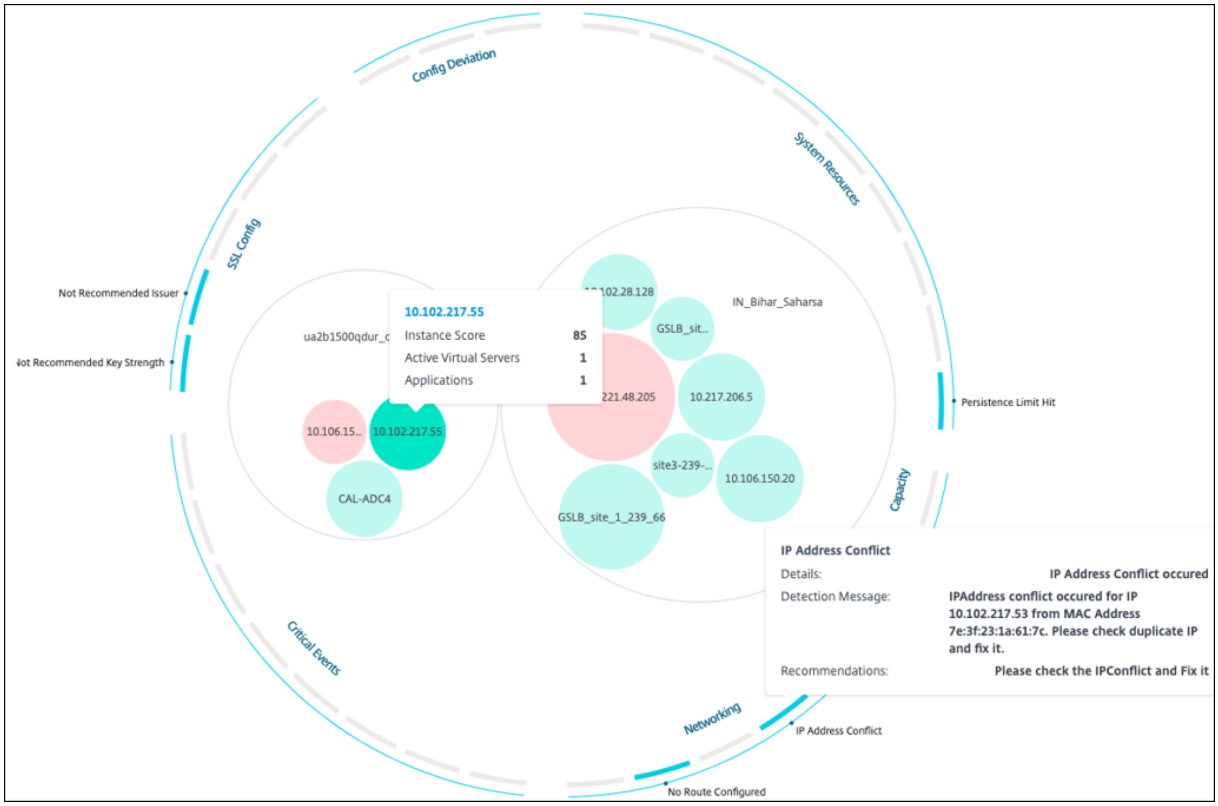
表格视图

您还可以使用 基础结构分析中的表格视图选项查看异常情况。导航到 基础结构 **>** 基础设施分析，然后单击 以显示所有托管实例。单击 › 以展开以了解详细信息。



查看异常的详细信息

例如，如果要查看网络中 **IP** 地址冲突 的详细信息，请单击 IP 地址冲突显示的异常。



- 详细信息 -指示检测到的异常
- 检测消息 -指示 IP 地址发生冲突的 MAC 地址
- 建议 -指示解决此 IP 地址冲突的故障排除过程

实例管理

September 2, 2024

实例是 Citrix Application Delivery Controller (ADC) 设备，您可以使用 NetScaler 控制台对其进行管理、监视和故障排除。向 NetScaler 控制台添加实例以对其进行监视。在设置 NetScaler 控制台或更高版本时，也可以添加实例。将实例添加到 NetScaler 控制台后，系统会持续对它们进行轮询以收集信息，这些信息以后可用于解决问题或用作报告数据。

实例可以分组为静态组或私有 IP 块。当您想要运行特定任务（如配置作业和其他任务）时，静态实例组可能非常有用。私有 IP 块根据实例的地理位置对实例进行分组。

添加实例

您可以在首次设置 NetScaler 控制台服务器时添加实例，也可以在以后添加实例。要添加实例，您必须指定每个 NetScaler 实例的主机名或 IP 地址，或指定 IP 地址范围。

要了解如何向 NetScaler 控制台添加实例，请参见向 NetScaler 控制台添加实例。

当您将实例添加到 NetScaler 控制台服务器时，服务器会隐式地将自己添加为该实例的陷阱目标并收集该实例的清单。要了解更多信息，请参阅 NetScaler 控制台如何发现实例。

添加实例后，您可以通过导航到 基础结构 **>** 实例 并选择实例类别将其删除。然后，选择要删除的实例，然后单击 R**em**ove（删除）。

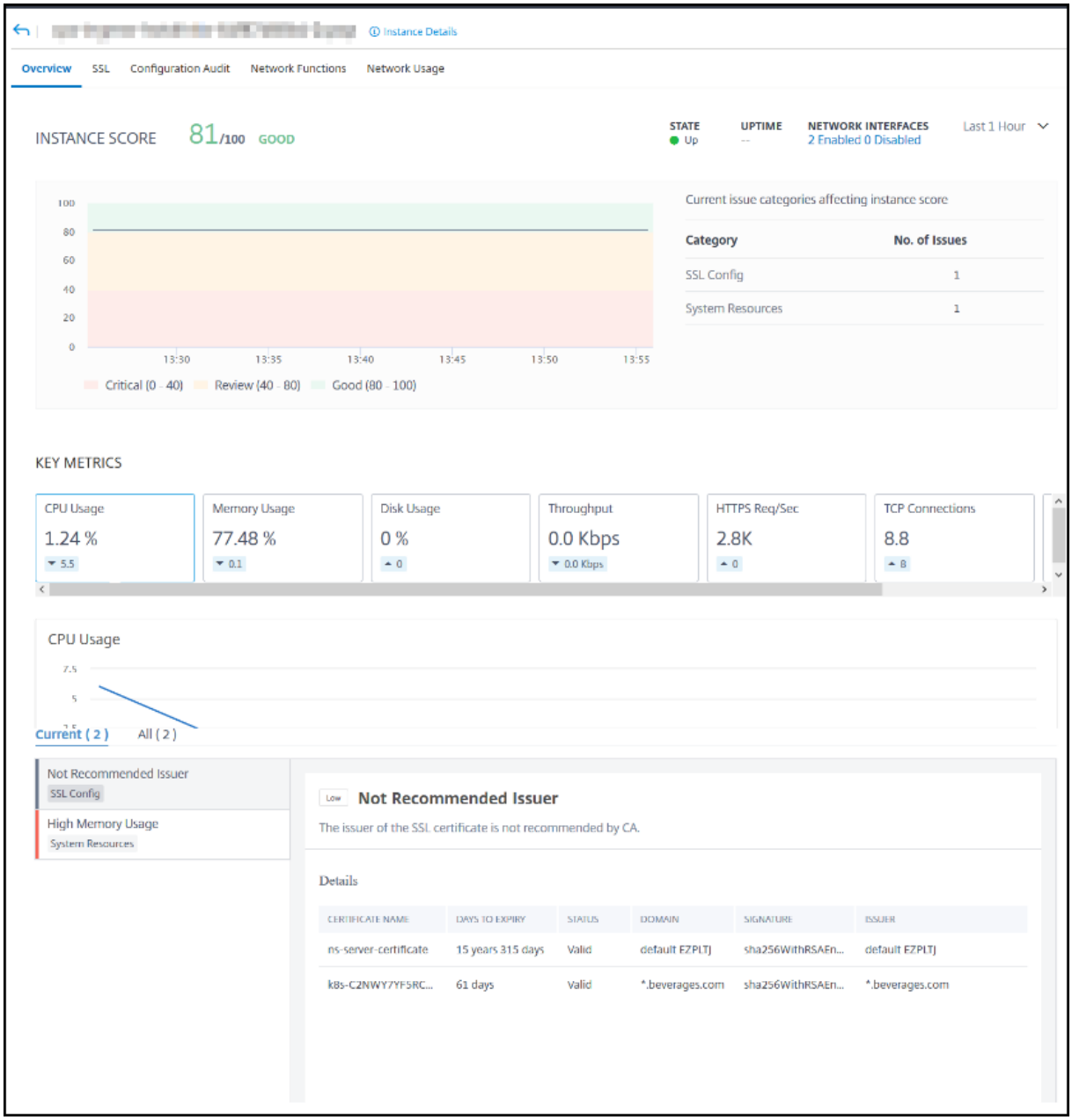
如何使用实例控制面板

NetScaler 控制台中的每实例控制面板以表格和图形格式显示所选实例的数据。在轮询过程中从您的实例收集的数据显示在控制面板上。

默认情况下，每分钟轮询托管实例以进行数据收集。使用 NITRO 调用持续收集状态、每秒 HTTP 请求、CPU 使用率、内存使用率和吞吐量等统计信息。作为管理员，您可以在单个页面上查看所有这些收集的数据，确定实例中的问题，并立即采取措施来纠正这些问题。

要查看特定实例的控制板，请导航到 基础结构 **>** 实例 **> NetScaler**。在 NetScaler 页面上，选择实例类型，然后选择要查看的实例，然后单击 控制板。

下图概述了每个实例控制板上显示的各种数据：



- 概述。概述选项卡显示所选实例的 CPU 和内存使用情况。您还可以查看实例生成的事件和吞吐量数据。此处还会显示特定于实例的信息，例如 IP 地址、其硬件和 LOM 版本、配置文件详细信息、序列号、联系人和其他信息。通过进一步向下滚动，您所选实例上可用的许可功能及其上配置的模式。有关更多信息，请参阅 实例详情。
- **SSL** 控制板。您可以使用每实例控制面板上的 SSL 选项卡来查看或监视所选实例的 SSL 证书、SSL 虚拟服务器和 SSL 协议的详细信息。您可以单击图表中的“数字”以显示更多细节。
- 配置审核。您可以使用配置审核选项卡查看所选实例上发生的所有配置更改。控制板上的 **NetScaler** 配置保存状态和 **NetScaler** 配置偏差图显示了与未保存的配置 相比保存的配置更改的高级详细信息。
- 网络功能。使用网络功能控制板，您可以监视在所选 NetScaler 实例上配置的实体的状态。您可以查看显示客户端连接、吞吐量和服务器连接等数据的虚拟服务器的图表。

- 网络使用情况。您可以在网络使用情况选项卡上查看所选实例的网络性能数据。您可以显示一小时、一天、一周或一个月的报告。时间轴滑块功能可用于自定义正在生成的网络报告的持续时间。默认情况下，仅显示八份报告，但您可以单击屏幕右下角的“加号”图标添加另一份绩效报告。

如何监视分布全球的站点

June 7, 2024

作为网络管理员，您可能必须监视和管理部署在不同地理位置的网络实例。但是，在分布在地理位置上的数据中心管理网络实例时，要衡量网络的要求并不容易。

NetScaler 控制台中的地理地图可为您提供站点的图形表示，并按地理位置细分您的网络监视体验。通过 Geomap，您可以按位置呈现网络实例分布，并监视网络问题。

以下各节说明如何在 NetScaler 控制台中监视数据中心。

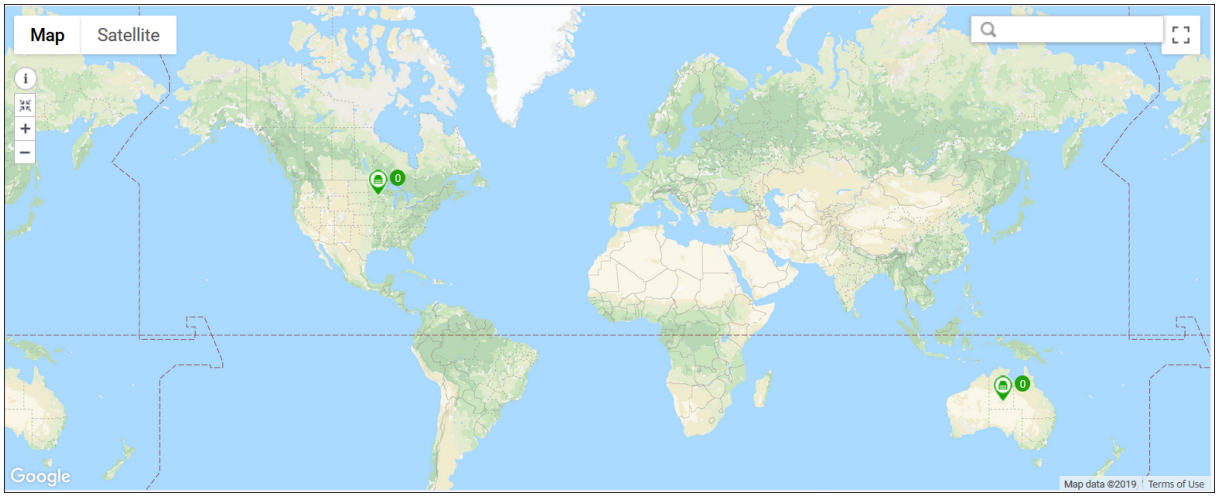
在 **NetScaler** 控制台中监视全球分布的站点

NetScaler 控制台站点是特定地理位置的 Citrix Application Delivery Controller (NetScaler) 实例的逻辑分组。例如，当一个站点被分配给 Amazon Web Services (AWS) 时，另一个站点可能被分配给 Azure™。还有另一个网站托管在租户的场所内。NetScaler 控制台管理和监视连接到所有站点的所有 NetScaler 实例。您可以使用 NetScaler 控制台监视和收集系统日志、AppFlow、SNMP 以及源自托管实例的任何此类数据。

NetScaler 控制台中的地理地图可为您提供站点的图形表示。Geomaps 还会按地理位置细分您的网络监视体验。通过地理图，您可以按位置可视化您的网络实例分布并监视所有网络问题。您可以单击菜单上的 基础结构，这将显示 实例控制板，直观地显示在世界地图上创建的站点。

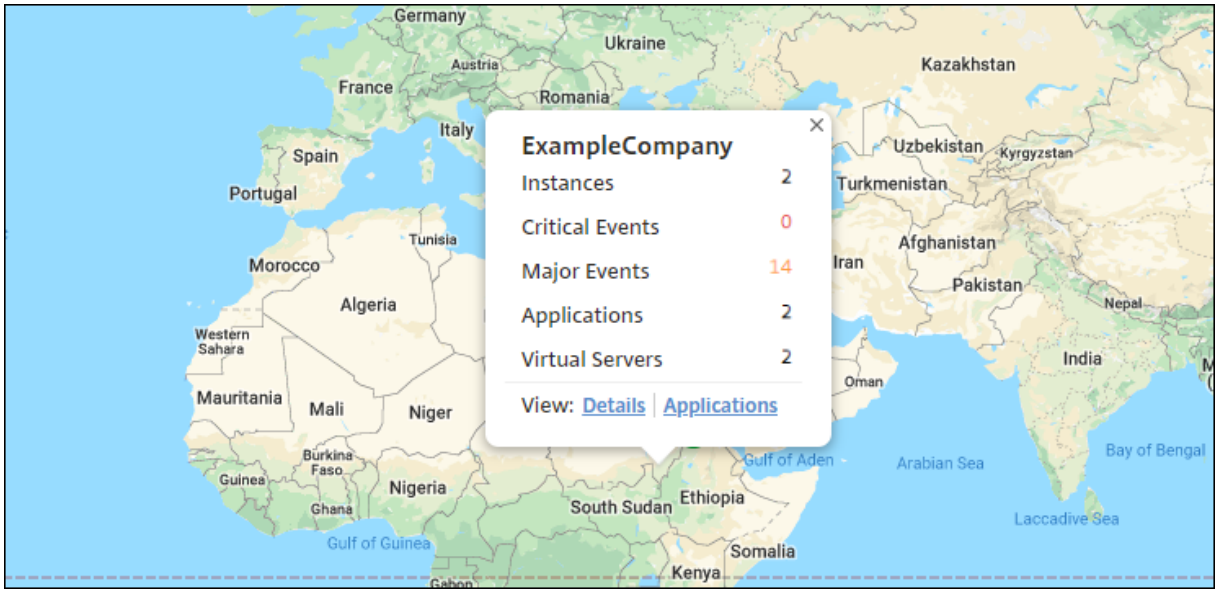
用例

一家领先的移动运营商公司 ExampleCompany 依靠私有服务提供商来托管其资源和应用程序。该公司已经有两个基地——一个位于美国的明尼阿波利斯，另一个在澳大利亚的爱丽斯泉。在此图中，您可以看到两个标记代表两个现有站点。



这些标记还显示站点上以下组件的计数：

- 实例：表示可用实例的数量。
- 应用程序：表示托管的应用程序数量。
- 虚拟服务器：指示可用虚拟服务器的数量。
- 严重事件：指示实例上发生的关键事件的计数。
- 重大事件：表示实例上发生的重大事件的数量。



单击 应用程序 以查看在每个站点中创建的所有自定义应用程序。

单击“详细信息”查看在每个站点中添加的 NetScaler 实例列表。单击选项卡以查看详细信息：

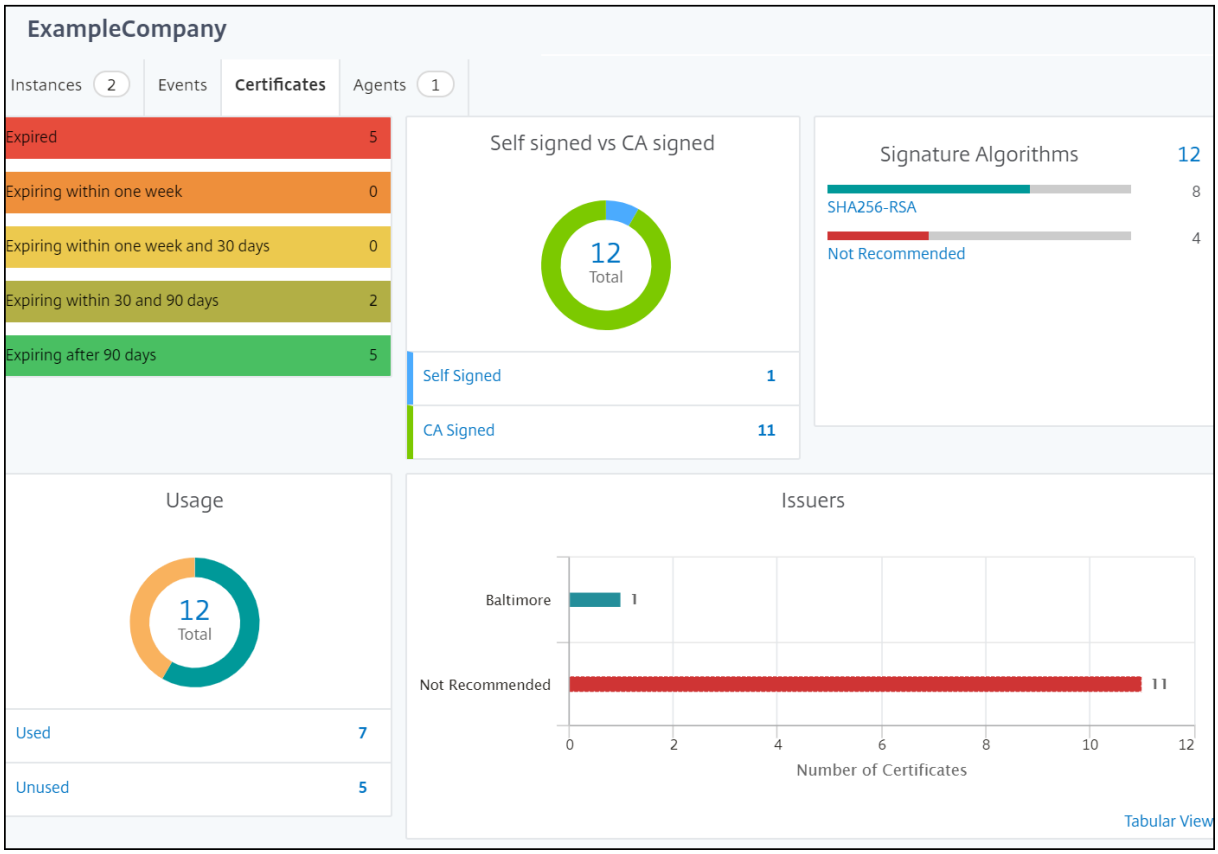
- “实例”选项卡：在此选项卡中查看以下内容：
  - 每个网络实例的 IP 地址

  - NetScaler 实例的类型
  - 关键事件的数量
  - 在 NetScaler 实例上引发的重大事件和所有事件。

- “事件”选项卡：查看实例上引发的关键和重要事件列表。
- “证书”选项卡：在此选项卡中查看以下内容：

  - 所有实例的证书列表
  - 到期状态
  - 重要信息以及许多正在使用的证书中排名前 10 位的实例。

- 代理选项卡：查看绑定实例的代理列表。



配置地理地图

ExampleCompany 决定在印度班加罗尔创建第三个站点。该公司希望通过将一些不太重要的内部 IT 应用程序转移到班加罗尔办公室来测试云。该公司决定使用 AWS 云计算服务。

作为管理员，您必须首先创建一个站点，然后在 NetScaler 控制台中添加 NetScaler 实例。您还必须将实例添加到站点，添加代理，并将代理绑定到站点。然后，NetScaler 控制台会识别 NetScaler 实例和代理所属的站点。

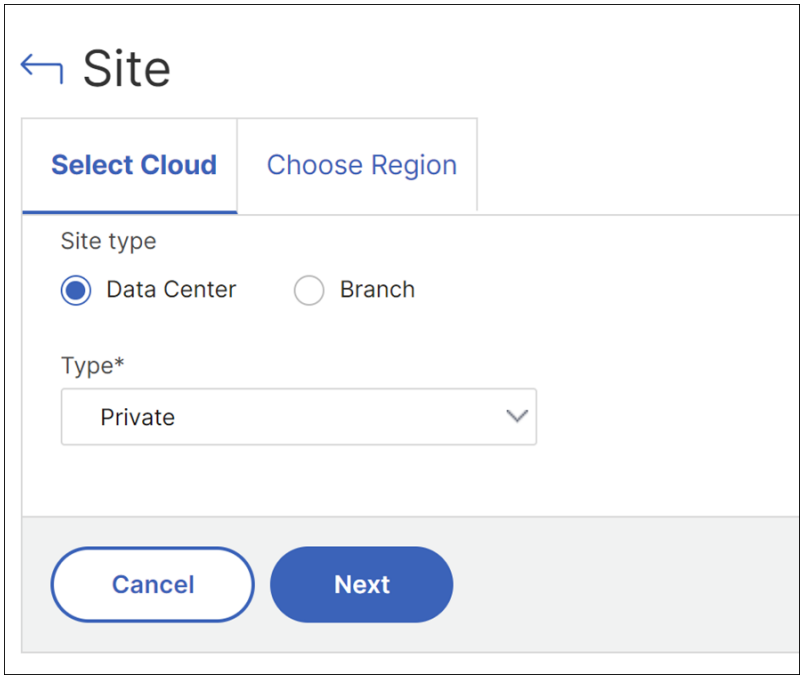
有关添加 NetScaler 实例的更多信息，请参阅添加实例。

创建站点

在 NetScaler 控制台中添加实例之前，请先创建站点。提供位置信息可让您精确定位站点。

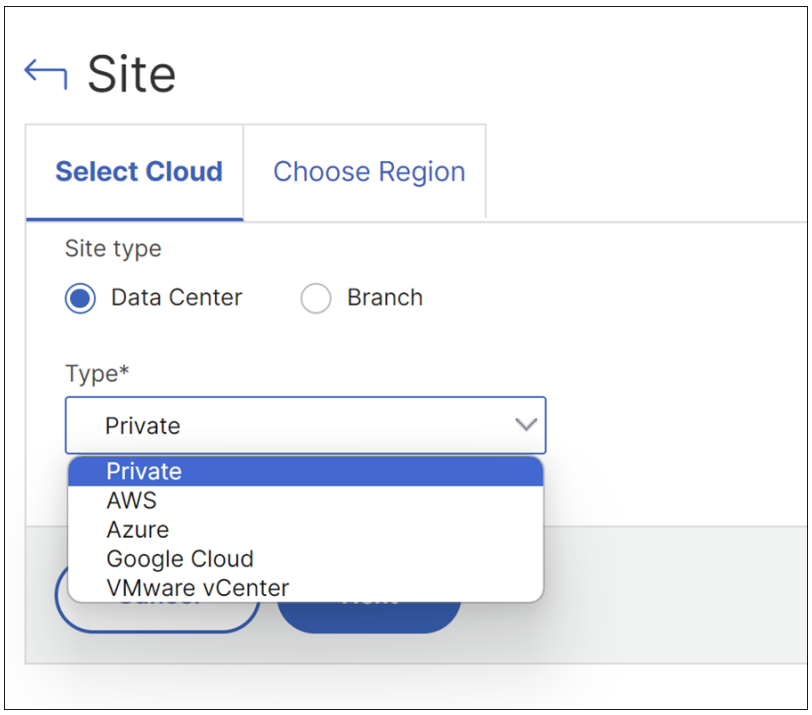
要创建站点，请执行以下操作：

1. 导航到基础架构 **>** 实例 **>** 站点。单击添加。
2. 在“选择云”选项卡上，选择站点类型。您可以创建数据中心或分支机构的站点。



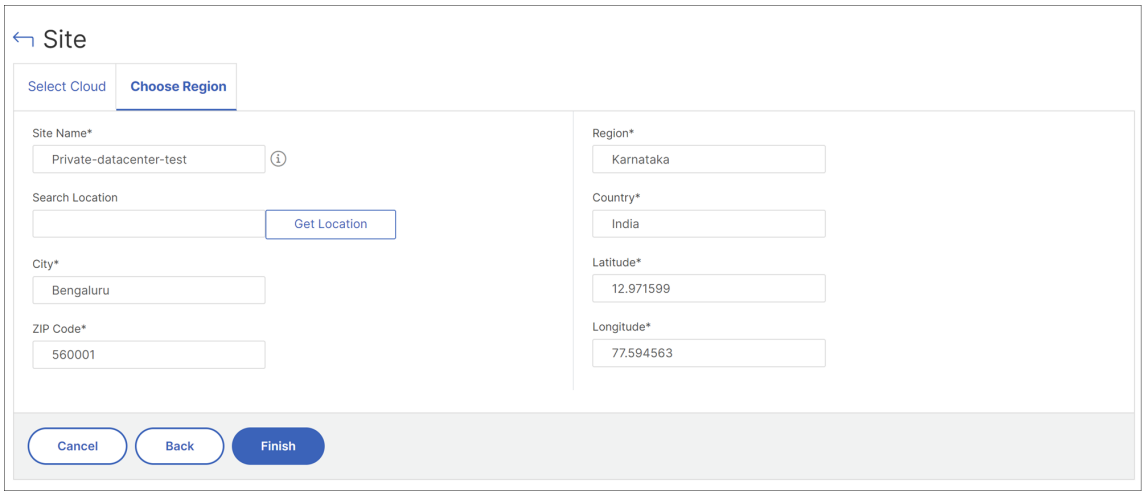
对于数据中心站点类型，请从列表中选择类型：

- 专用
- AWS
- Azure
- Google Cloud
- VMware vCenter



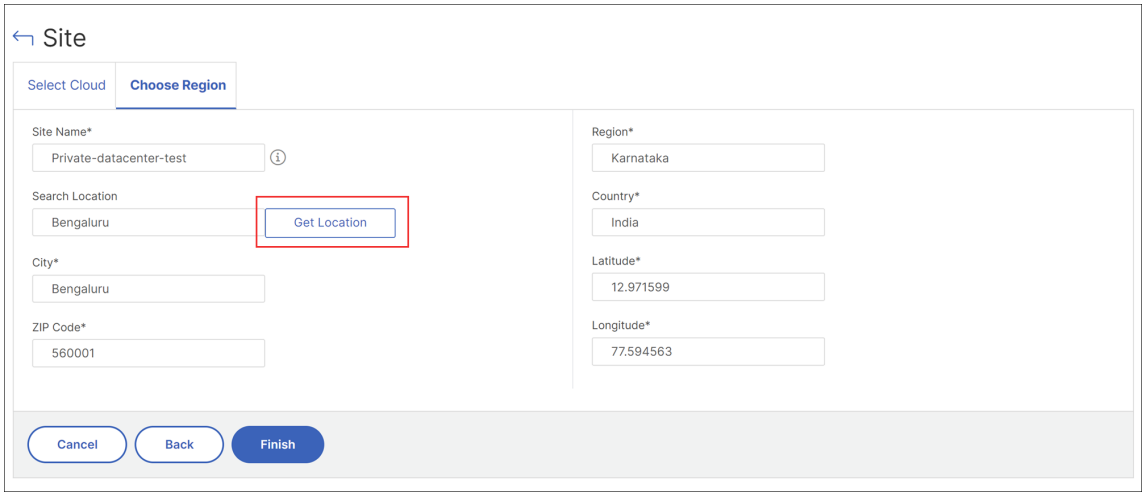
3. 单击下一步。
4. 在“选择区域”选项卡上，输入以下详细信息：

   - 站点名称
   - 城市
   - 邮政编码
   - 地理区域
   - 国家/地区
   - 纬度
   - 经度



或者，您可以在“搜索位置”中输入位置，然后单击“获取位置”以精确定位该站点。“城市”、“邮政编码”、“地

区”、“国家”、“纬度”和“经度”字段将自动填充。



5. 单击完成。

> 备注：
>
> 概述的步骤适用于：
>
> - 分支机构站点类型。
> - 私有类型的数据中心站点类型。
> - 当未为云提供商类型选择提取选项时。

为云提供商类型创建站点

您可以使用云提供商类型创建站点，然后选择启用还是禁用“提取”选项。默认情况下，未选择“提取”选项。

提取选项仅适用于 AWS、Azure 和 Google Cloud 平台。

有关为特定云提供商创建网站的详细说明，请参阅以下部分：

1. 在 AWS 中创建网站
2. 在 Azure 中创建站点
3. 在 Google Cloud 中创建网站
4. 在 VMware vCenter 中创建站点

编辑站点

要修改现有站点，请执行以下操作：

1. 选择该站点，然后单击“编辑”。
2. 在“配置站点”页面上，您可以更新站点类型。例如，如果您之前选择了分支机构，则可以更新到数据中心。
3. 根据站点类型，您可以修改类型。例如，您可以从列表中将类型从私有数据中心更改为公有云。

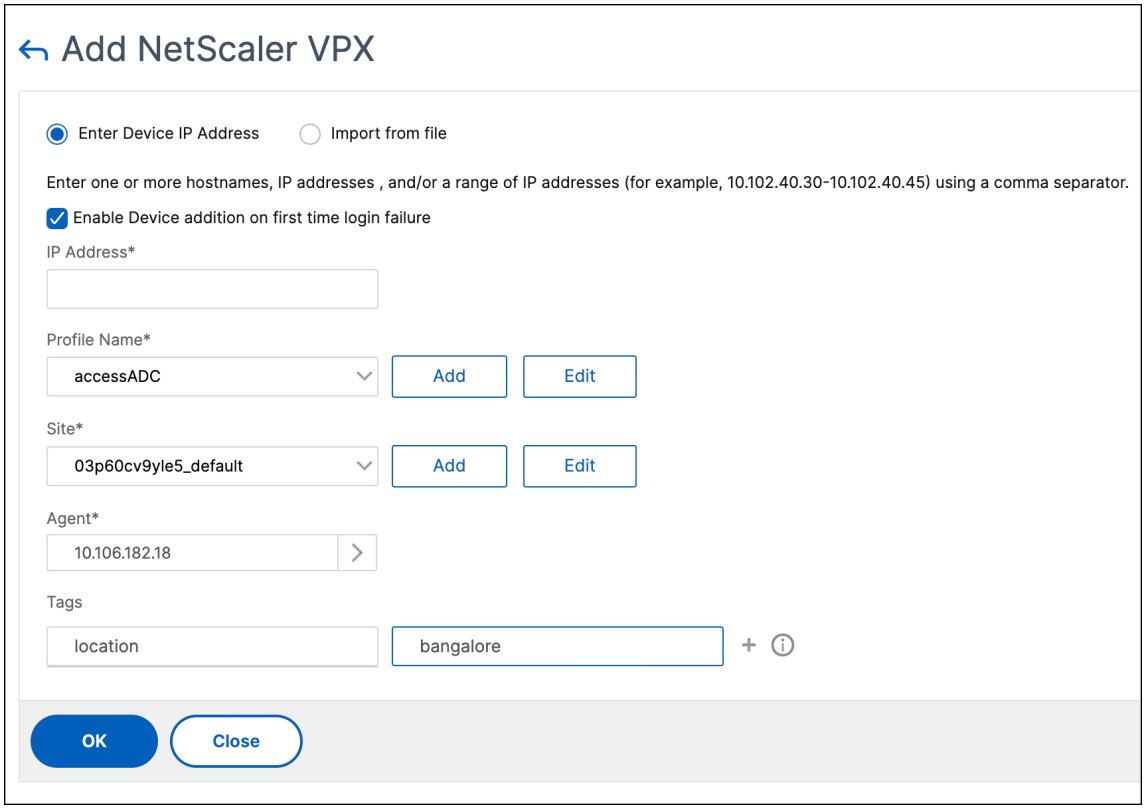
删除站点

1. 要删除站点，请选择该站点并单击“删除”。
2. 在“确认”页面上，单击“是”。

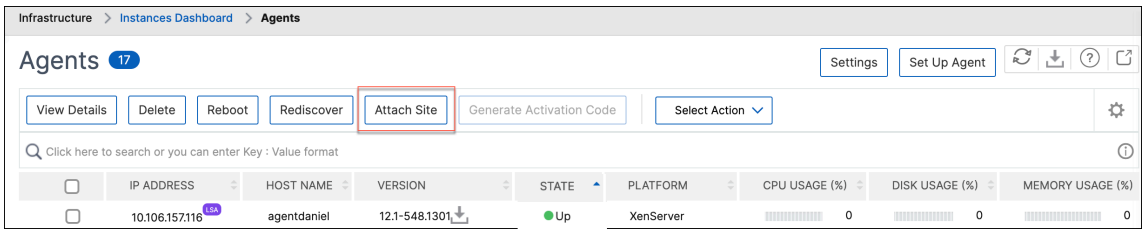
要添加实例并选择站点，请执行以下操作：

创建站点后，必须在 NetScaler 控制台中添加实例。您可以选择先前创建的站点，也可以创建站点并关联实例。

1. 在 NetScaler 控制台中，导航到基础架构 **>** 实例 **> NetScaler**。
2. 选择 **VPX**，然后单击“添加”。
3. 在 添加 **NetScaler VPX** 页面上，键入 IP 地址并从列表中选择配置文件。
4. 从列表中选择站点。您可以单击“站 点”字段旁边的“添加”按钮来创建站点，或者单击“编辑”按钮以更改默认站点的详细信息。
5. 单击向右箭头，然后从显示的列表中选择座席。



6. 选择代理后，您必须将代理与站点关联。此步骤允许代理绑定到站点。选择代理并单击 附加站点。



a) 从列表中选择站点，然后单击保存。

7. 或者，您可以输入 标签的键和值字段。
8. 单击确定。

您还可以通过导航到 基础结构 **>** 实例 **>** 代理将代理附加到站点。

要将代理与站点关联，请执行以下操作：

1. 在 NetScaler 控制台中，导航到基础架构 **>** 实例 **>** 代理。
2. 选择代理，然后单击“附加站点”。
3. 您可以关联网站并单击保存。

NetScaler 控制台开始监视在班加罗尔站点中添加的 NetScaler 实例以及其他两个站点的实例。

要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

> 注意：
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

如何创建标记并分配给实例

January 29, 2024

NetScaler 控制台现在允许您将 NetScaler 实例与标签关联起来。标签是您可以分配给实例的关键字或单词术语。这些标签添加了有关实例的一些其他信息。可以将标签视为有助于描述实例的元数据。标签允许您根据这些特定关键字对实例进行分类和搜索。您还可以将多个标签分配给单个实例。

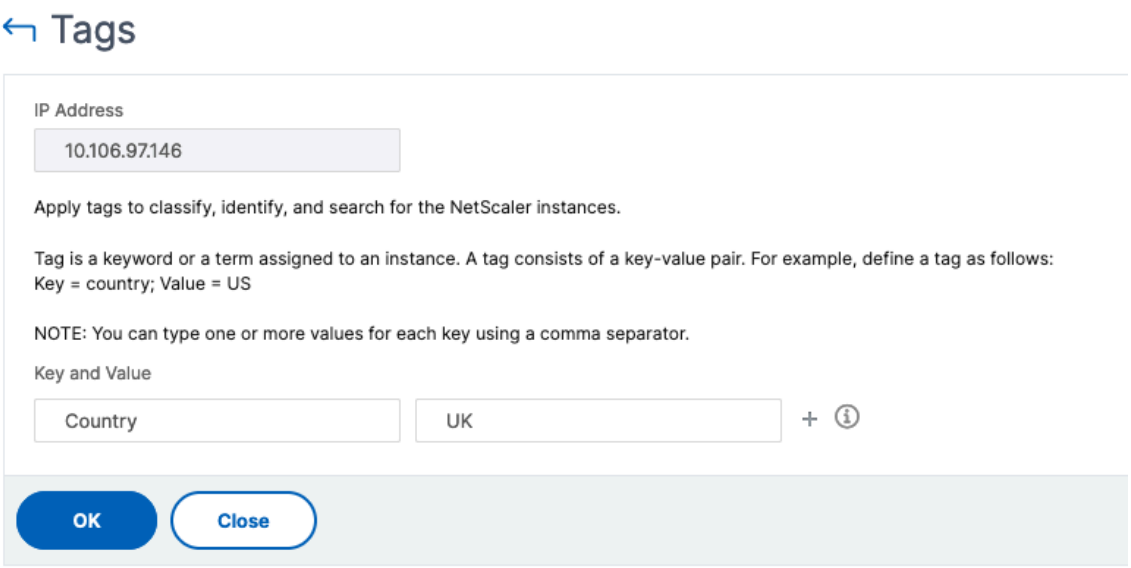
以下用例可帮助您了解对实例进行标记将如何帮助您更好地监视实例。

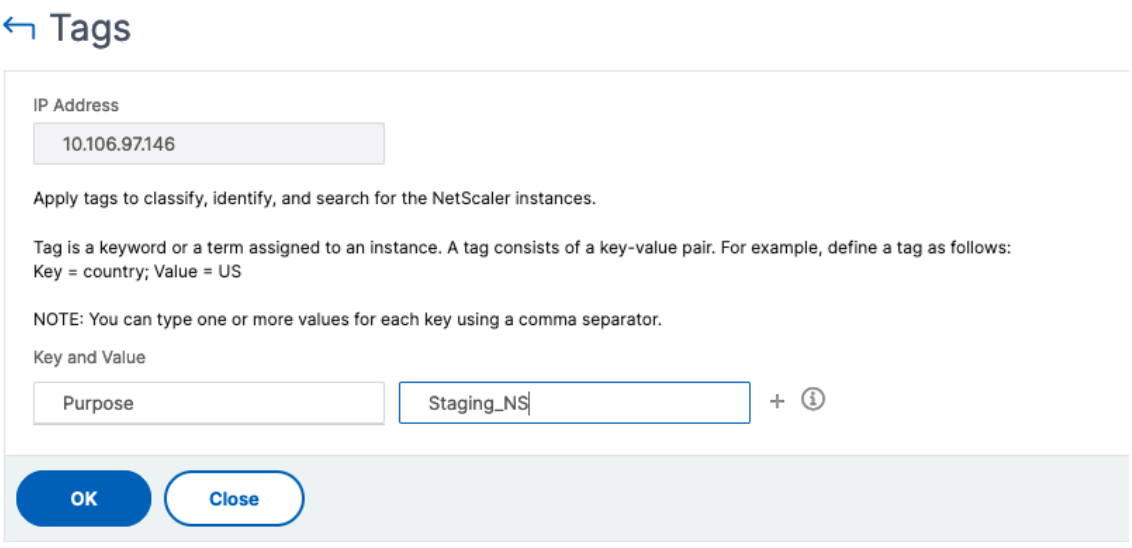
- 使用案例 **1**：您可以创建标记来标识位于英国的所有实例。在这里，您可以创建一个标签，密钥为“国家/地区”，值为“UK”。此标签可帮助您搜索和监视位于英国的所有实例。
- 使用案例 **2**：您要搜索处于临时环境中的实例。在这里，您可以创建一个标签，其中密钥为“目的”，值为 Staging_NS。此标记可帮助您将正在暂存环境中使用的所有实例与运行客户端请求的实例隔离开来。
- 使用案例 **3**：考虑一种情况，您想要查找位于英国 Swindon 区域并由您拥有的 NetScaler 实例列表。您可以为所有这些要求创建标签，然后将其分配给满足这些条件的所有实例。

要为 **NetScaler VPX** 实例分配标签，请执行以下操作：

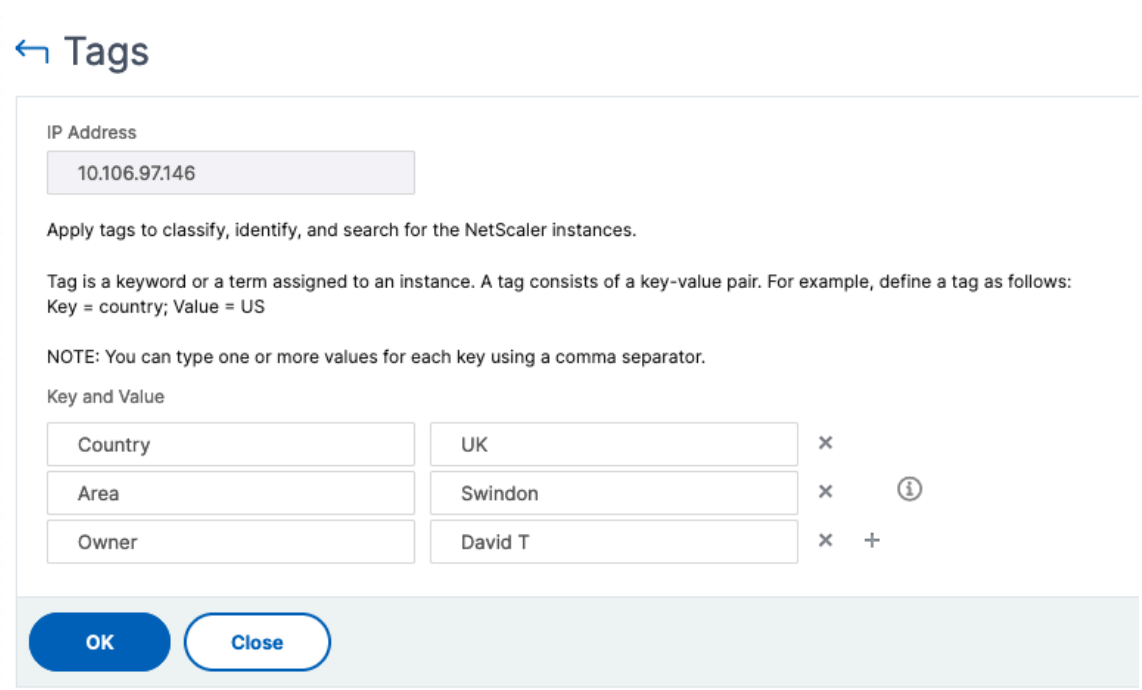
1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例 **> NetScaler**。
2. 选择 **VPX** 选项卡。
3. 选择所需的 VPX 实例。
4. 单击“标签”。出现的“标签”窗口允许您通过为创建的每个关键字分配值来创建自己的“键值”对。

   例如，下图显示了创建的几个关键字及其值。您可以添加自己的关键字并为每个关键字键入一个值。



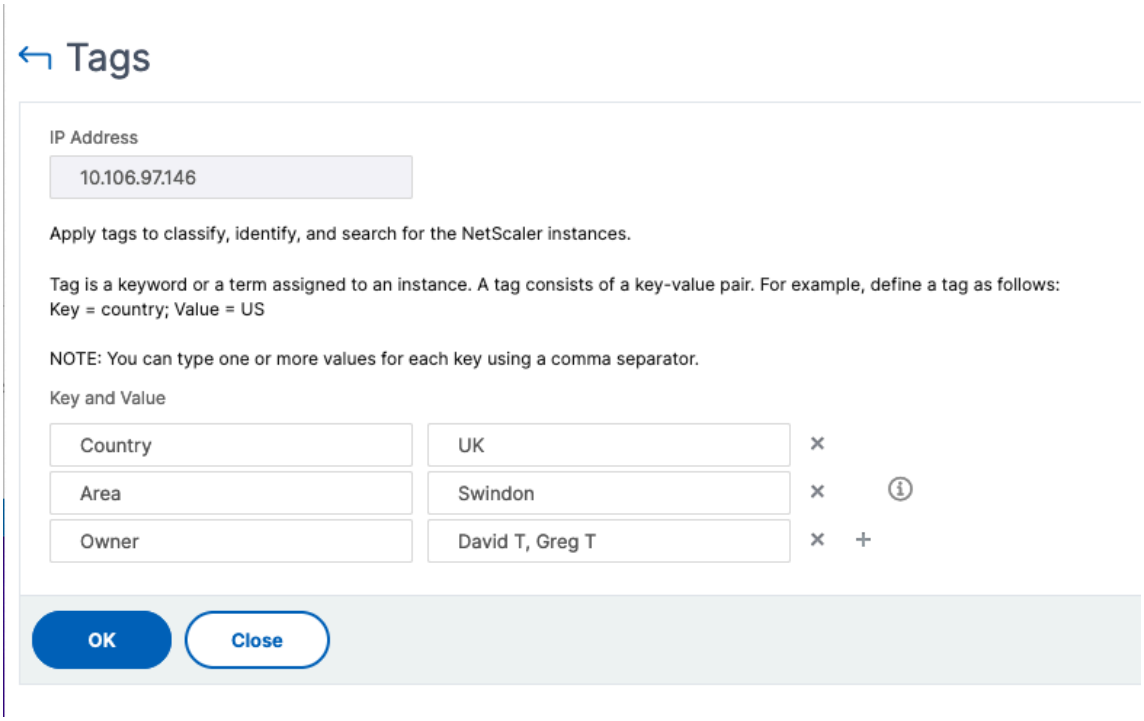


您也可以点击“+”添加多个标签。通过添加多个有意义的标签，您可以高效地搜索实例。



您可以通过用逗号分隔来向关键字添加多个值。

例如，您要将管理员角色分配给另一位同事 Greg T。您可以添加用逗号分隔的他的姓名。添加多个名称可帮助您按其中一个名称或两个名称进行搜索。NetScaler 控制台将逗号分隔的值识别为两个不同的值。



要详细了解如何根据标签搜索实例，请参阅 如何使用标签和属性的值搜索实例。

5. 单击确定。

> 注意
>
> 您以后可以添加新标签或删除现有标签。您创建的标签数量没有限制。

如何使用标记和属性的值搜索实例

January 29, 2024

在某些情况下，NetScaler 控制台正在管理许多 NetScaler 实例。作为管理员，您可能希望灵活地根据特定参数搜索实例清单。NetScaler 控制台现在提供了改进的搜索功能，可以根据您在搜索字段中定义的参数来搜索 NetScaler 实例的子集。您可以根据两个标准（标签和属性）搜索实例。

- 标签。标签是您可以分配给 NetScaler 实例的术语或关键字，以添加有关 NetScaler 实例的其他描述。现在，您可以将您的 NetScaler 实例与标签相关联。这些标签可用于更好地识别和搜索 NetScaler 实例。
- 属性。在 NetScaler 控制台中添加的每个 NetScaler 实例都有一些与该实例相关的默认参数或属性。例如，每个实例都有自己的主机名、IP 地址、版本、主机 ID、硬件型号 ID 等。您可以通过为这些属性中的任何一个指定值来搜索实例。

例如，假设您想要找出版本为 12.0 且处于 UP 状态的 NetScaler 实例列表。在这里，实例的版本和状态由默认属性定义。

除了实例的 12.0 版本和 UP 状态外，您还可以搜索您拥有的那些实例。您可以创建一个“所有者”标签并为该标签分配一个值“David T”。有关如何创建和分配标签的更多信息，请参阅 如何创建标签并分配给实例。

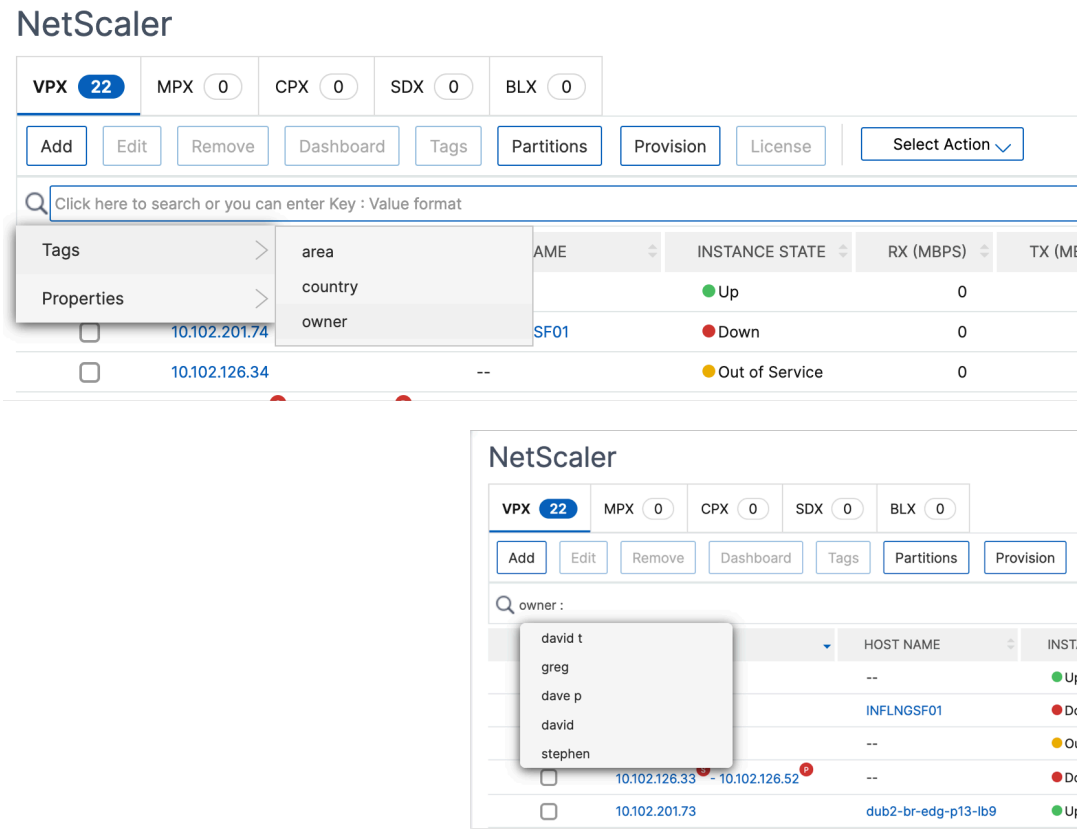
您可以使用标签和属性的组合来创建自己的搜索条件。

搜索 **NetScaler VPX** 实例

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例 **> NetScaler**。
2. 选择 **VPX** 选项卡。
3. 单击搜索字段。您可以使用标签或属性或将两者结合起来来创建搜索表达式。

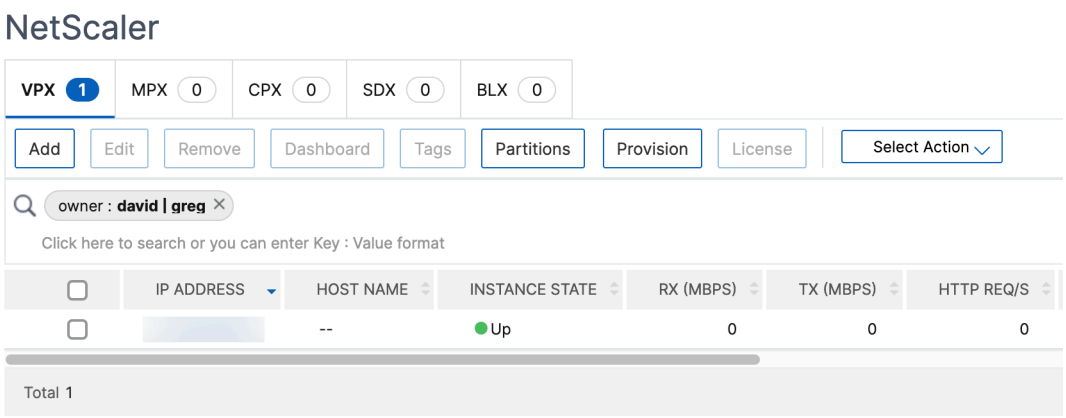
   以下示例显示如何有效地使用搜索表达式来搜索实例。

   a) 选择“标签”选项，然后选择“所有者”。选择“大卫 T”。

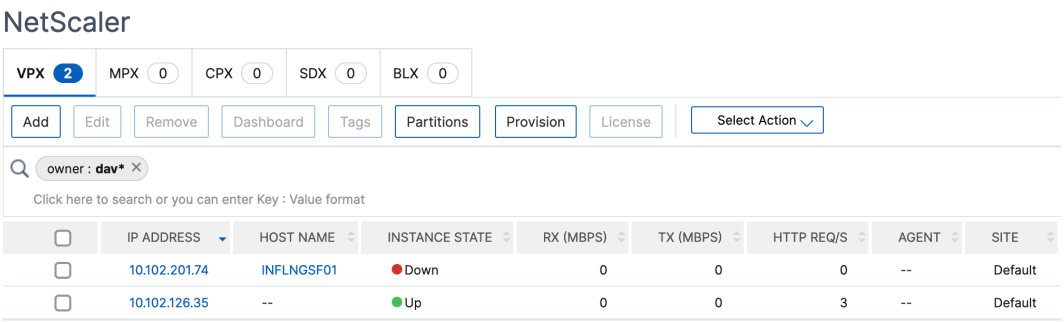


NetScaler 控制台支持搜索表达式中的正则表达式和通配符。

a) 您可以使用正则表达式来进一步扩展搜索条件。例如，您要搜索由 David 或 Stephen 拥有的实例。在这种情况下，您可以通过使用“|”表达式分隔值来键入值。



b) 您还可以使用通配符替换或表示一个或多个字符。例如，您可以键入 Dav* 以搜索“David”和“Dave P”拥有的所有实例。



> 注意：
>
> 有关正则表达式和通配符以及如何使用它们的更多信息，请单击搜索栏中的“信息”图标。

管理 **NetScaler** 实例的管理分区

January 29, 2024

您可以在 Citrix 应用程序 Delivery Controller (NetScaler) 实例上配置管理分区，以便在同一 NetScaler 实例上为组织中的不同组分配不同的分区。您可以分配网络管理员来管理多个 NetScaler 实例上的多个分区。

NetScaler 控制台提供了一种从单个控制台无缝管理管理员拥有的所有分区的方法。您可以在不中断其他分区配置的情况下管理这些分区。

要允许多个用户管理不同的管理分区，您必须创建组，然后将用户和分区分配给这些组。有关创建组或用户的更多信息，请参阅 创建用户 和 创建组。

用户只能查看和管理其所属组中的分区。当您发现 NetScaler 实例时，在该 NetScaler 实例上配置的管理分区会自动添加到系统中。在 NetScaler 控制台中，每个管理分区都被视为一个实例。

查看管理员分区

假设您有两个 NetScaler VPX 实例，并且在每个实例上配置了两个管理分区。例如，NetScaler 实例 10.xx.xx.100 有分区 1 和分区 2，10.xx.xx.101 实例有第一个分区和第二个分区。

执行以下步骤查看管理分区：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 在 **VPX** 选项卡中，单击“分区”。

例如，如果您在以下条件下创建组：

- 在“设置” **>** “用户和角色” **>** “创建组” **>** “授权设置” **>** “选择实例”中，选择“10.xx.xx.100-partition-1”和“10.xx.xx.101-第一个分区”实例。

- 您将“User1”分配给该组。

User1 只能查看和管理添加到该组的那些分区。但是，未添加到该组的分区即使属于相同的实例，也仅限于用户使用。

在此示例中，10.xx.xx.100-partition-2 和 10.xx.xx.101 秒的分区受到限制，因为这些实例未添加到分配用户的组中。

如果您想让其他用户管理管理分区 10.xx.xx.100-partition-2 和 10.xx.xx.101 秒分区，请创建具有以下条件的组：

- 在“授权设置”选项卡中，选择 10.xx.xx.100-partition-2 和 10.xx.xx.101 秒的分区实例。
- 将所需的用户分配到组。

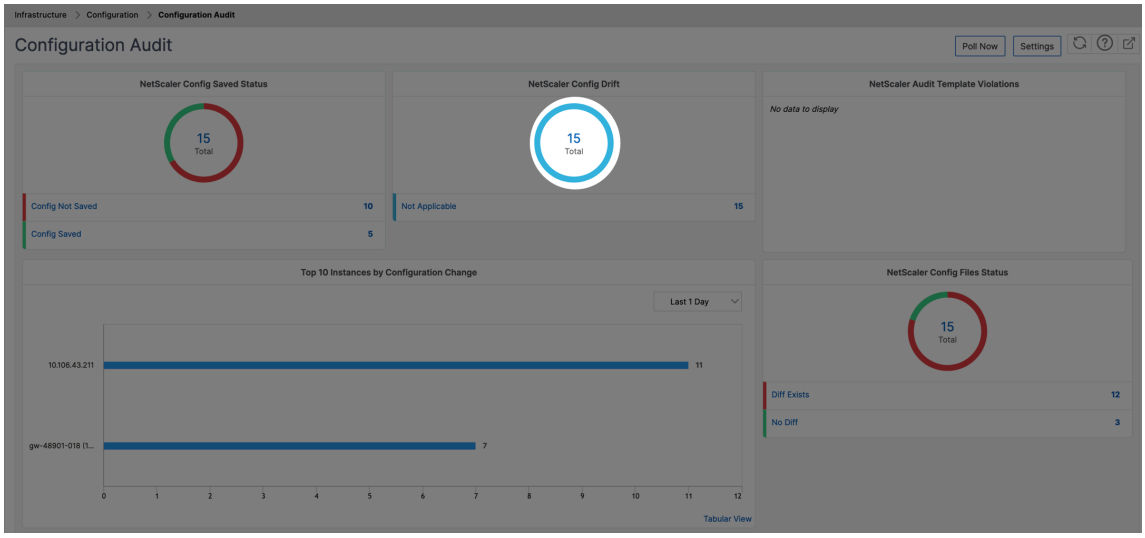
该组允许分配的用户查看和管理选定的管理分区。

查看修订历史记录差异

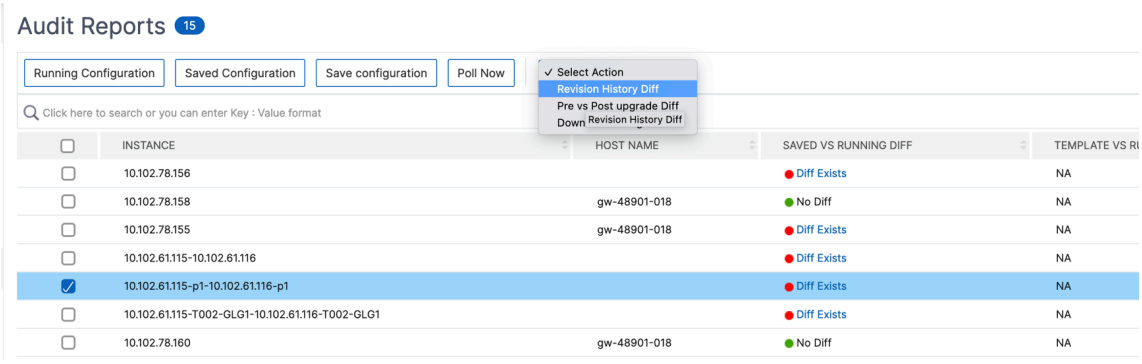
管理分区的修订历史记录差 异允许您查看分区 NetScaler 实例的五个最新配置文件之间的差异。您可以将配置文件相互比较（例如配置修订版本-1 配置修订版本-2），或与配置修订版本与当前运行/保存的配置进行比较。除了配置的差异外，还显示了校正配置。您可以将所有更正命令导出到本地文件夹并更正配置。

要查看修订历史记录差异，请执行以下操作：

1. 导航到基础架构 **>** 配置审核。配置审核控制板显示各种报告。单击圆环图中心显示的数字。

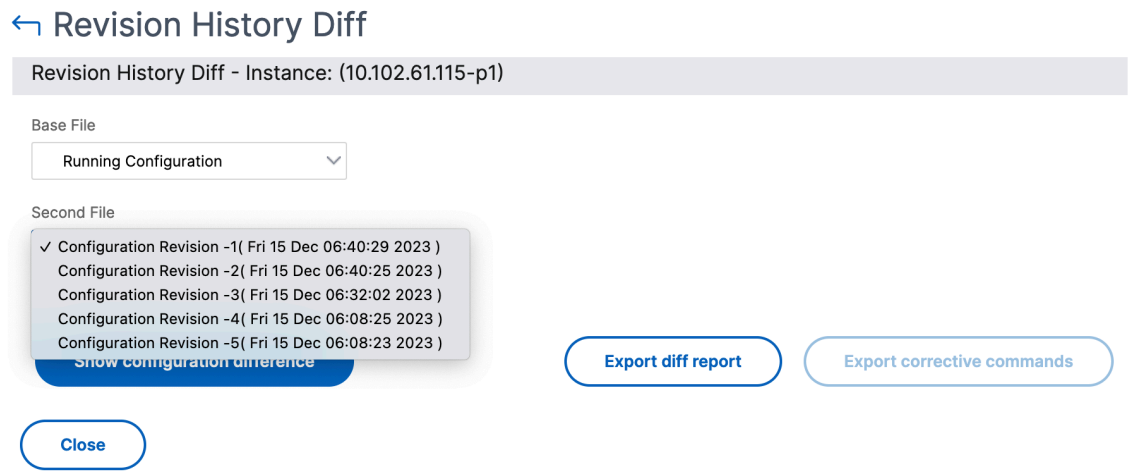


2. 选择已分区的 NetScaler 实例。
3. 从操作框中，单击 修订历史记录差异。

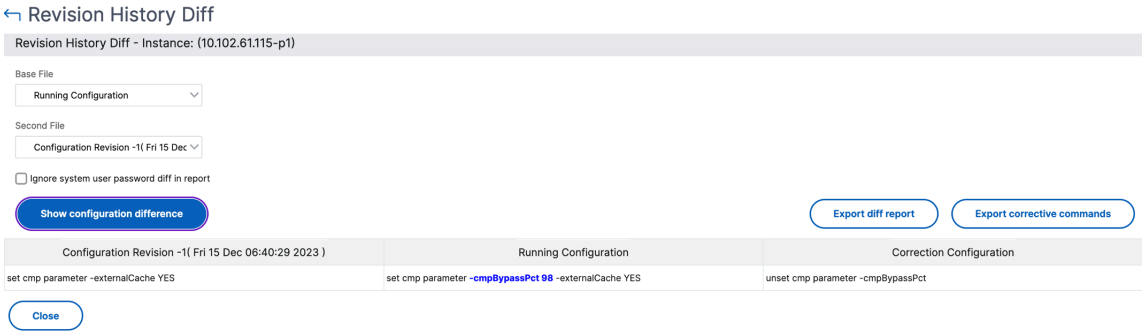


4. 在 修订历史记录差异 页面上，选择要比较的文件。例如，将“保存的配置”与“配置修订版 2”进行比较，然后单击“显示配置差异”。

   然后，您可以查看所选分区 NetScaler 实例的五个最新配置文件之间的差异。以下是管理分区的示例，其中保存了五种配置：

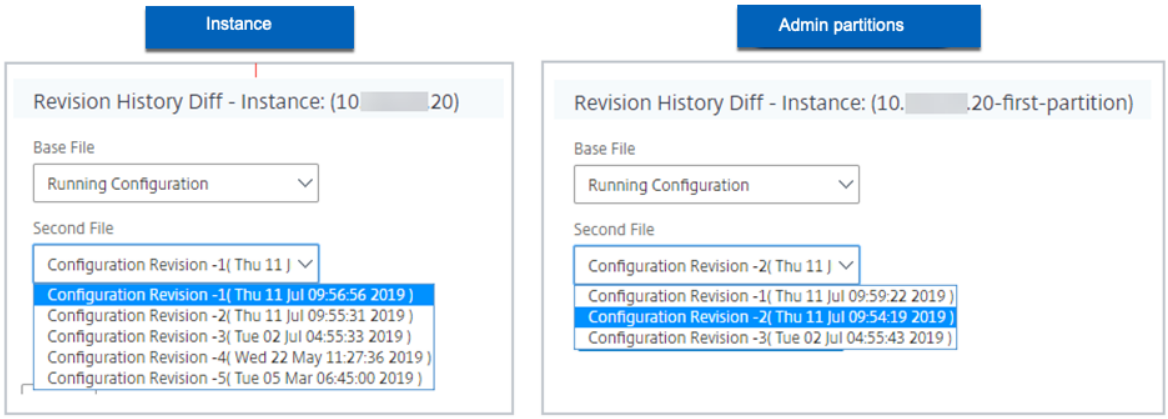


   您还可以查看更正配置命令并将这些更正命令导出到本地文件夹。这些纠正命令是需要在基础文件上运行的命令，才能使配置到所需状态（用于比较的配置文件）。



管理分区和实例上保存的配置不同。在以下示例中，10.xx.xx.20 实例具有五个保存的配置，其中此实例的管理分区具

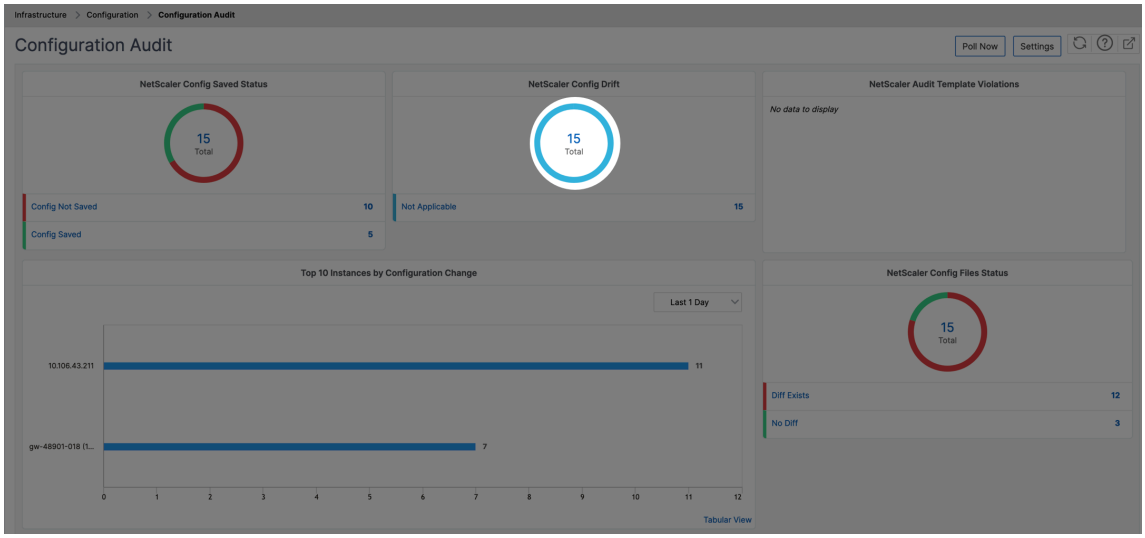
有三个不同的保存配置：



查看模板与运行差异

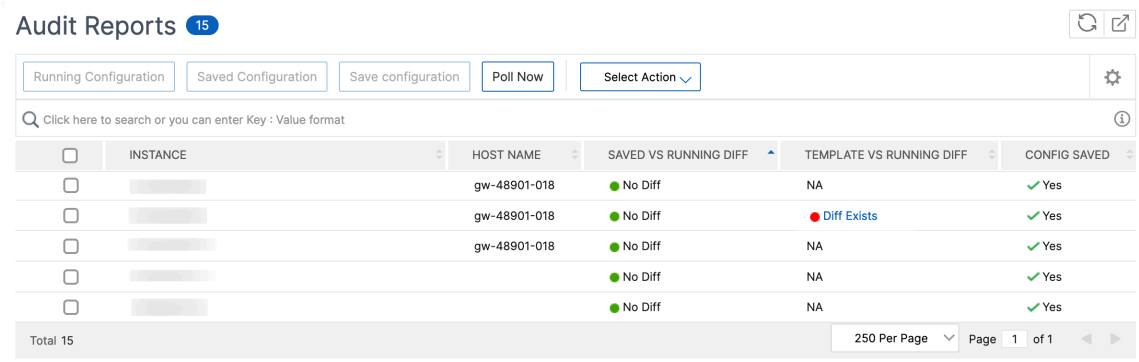
分区审核模板 允许您创建自定义配置模板并将其与分区实例关联。使用审核模板的实例运行配置中的任何变体都会显示在审核 报告页面的“模板与运行差异”列中。除了配置的差异外，还显示了校正配置。您还可以将所有更正命令导出到本地文件夹并更正配置。

1. 导航到基础架构 **>** 配置审核。配置审核控制板显示各种报告。单击圆环图中心显示的数字。



2. 在 审核报告 页中，单击“模板与运行 差异”列下的差异存在 超链接。

   如果审核模板和运行配置之间存在任何差异，则差异显示为超链接。单击超链接可查看差异（如果存在）。除了配置的差异外，还显示了校正配置。您还可以将所有更正命令导出到本地文件夹并更正配置。



要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

> 注意：
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

备份和还原 **NetScaler** 实例

January 29, 2024

您可以备份 Citrix Application Delivery Controller (NetScaler) 实例的当前状态，然后使用备份文件将 NetScaler 实例还原到相同状态。在升级实例之前或出于预防原因，您必须始终备份实例。稳定系统的备份使您能够将其恢复到稳定点，如果系统变得不稳定。有多种方法可以在 NetScaler 实例上执行备份和恢复。您可以使用 GUI、CLI 手动备份和恢复 NetScaler 配置，也可以使用 NetScaler 控制台执行自动备份和手动恢复。NetScaler 控制台使用 NITRO 调用以及安全外壳 (SSH) 和安全复制 (SCP) 协议来备份托管 NetScaler 实例的当前状态。

NetScaler 控制台创建完整备份并恢复以下 NetScaler 实例类型：

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

有关更多信息，请参见 备份和恢复 NetScaler 实例。

> 注意：
>
> - 在 NetScaler 控制台中，您无法在 NetScaler 群集上执行备份和还原操作。
> - 不能使用从一个实例创建的备份文件来还原另一个实例。

备份的文件作为压缩的 TAR 文件存储在以下目录中：

```
/var/mps/tenants/root/tenants/<specify-the-tenant-name>/device_backup/
```

为避免由于磁盘空间不可用而出现问题，您最多可以在此目录中保存三个备份文件。

要备份和恢复 NetScaler 实例，必须首先在 NetScaler 控制台上配置备份设置。配置设置后，您可以选择单个 NetScaler 实例或多个实例，然后在这些实例中创建配置文件的备份。如有必要，您还可以使用这些备份的文件还原 NetScaler 实例。

使用 **NetScaler** 控制台为选定的 **NetScaler** 实例创建备份

如果要备份选定的 NetScaler 实例或多个实例，请执行以下任务：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例。在“实例”下，选择要在屏幕上显示的实例类型（例如 VPX）。
2. 选择要备份的实例。
   - 对于 MPX、VPX 和 BLX 实例，从“选择 操作”列表中选择“备份/恢复”。
   - 对于 SDX 实例，请单击 备份/恢复。
3. 在 **Backup Files**（备份文件）页面上，单击 **Back Up**（备份）。
4. 指定是否加密备份文件以提高安全性。您可以输入密码，也可以使用之前在“实例备份设置”页面上指定的全局密码。
5. 单击继续。

将备份文件传输到外部系统

作为预防措施，您可以将备份文件的副本传输到另一个系统。当您要恢复配置时，必须先将备份文件上载到 NetScaler 控制台服务器，然后执行还原操作。

要传输 **NetScaler** 控制台备份文件，请执行以下操作：

1. 导航到 基础结构 **>** 实例 **> NetScaler** ，然后选择实例类型。例如，VPX。
2. 选择实例，然后从“选择操作”列表中选择“备份/恢复”。
3. 选择备份文件，然后单击 传输。

   此时将显示 传输备份文件 页面。指定以下参数：

a) 服务器 -要将备份文件传输到的系统的 IP 地址。

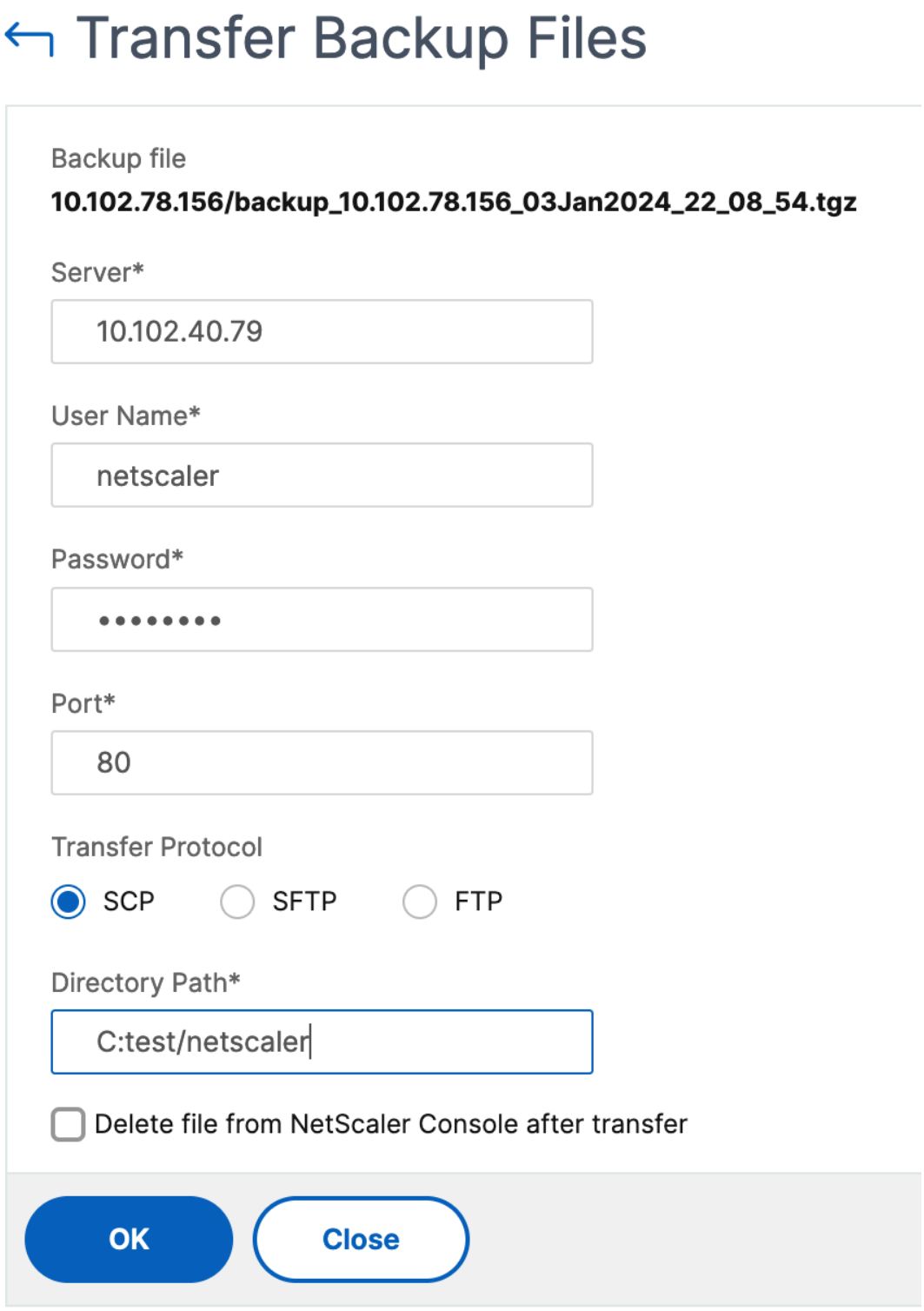
b) 用户名 和 密码—正在复制备份文件的新系统的用户凭据。

c) 端口—要将文件传输到的系统的端口号。

d) 传输协议 -用于进行备份文件传输的协议。您可以选择 SCP、SFTP 或 FTP 协议来传输备份文件。

e) 目录路径—备份文件在新系统上载输到的位置。

f) 单击确定。



注意：

来自 NetScaler 控制台服务的备份文件通过代理发送到外部服务器。如果有许多代理，NetScaler 备份文件将通

> 过用于添加 NetScaler 实例的同一个代理发送。要详细了解与代理相关的实例，请导航到 基础架构 **> NetScaler** 代理。

使用 **NetScaler** 控制台恢复 **NetScaler** 实例

> 注意：
>
> 如果您的 HA 对中有 NetScaler 实例，则需要注意以下几点：
>
> - 恢复创建备份文件的同一个实例。例如，让我们考虑一下从 HA 对的主实例中获取备份的情况。在还原过程中，确保您恢复的是同一个实例，即使它不再是主实例。
> - 当您在主 NetScaler 实例上启动还原过程时，您将无法访问主实例，辅助实例将更改为 **STAYSECONDARY**。主实例上的还原过程完成后，辅助 NetScaler 实例将 从 **STAYSECONDARY** 模式更改为 **ENABLED** 模式，并再次成为 HA 对的一部分。在还原过程完成之前，您可以预期主实例可能会停机。

执行以下任务，使用您之前创建的备份文件恢复 NetScaler 实例：

1. 导航到 基础结构 **>** 实例，选择要恢复的实例，然后单击 查看备份。
2. 在“备份文件”页面上，选择包含要还原的设置的备份文件，然后单击“恢复”。

使用 **NetScaler** 控制台恢复 **NetScaler SDX** 设备

在 NetScaler 控制台中，NetScaler SDX 设备的备份包括以下内容：

- 设备上托管的 NetScaler 实例
- SVM SSL 证书和密钥
- 实例删除设置（XML 格式）
- 实例备份设置（XML 格式）
- SSL 证书轮询设置（XML 格式）
- SVM 数据库文件
- SDX 上存在的设备的 NetScaler 配置文件
- NetScaler 构建映像
- NetScaler XVA 图像，这些图像存储在以下位置：
  `/var/mps/sdx_images/`
- SDX 单捆绑包映像 (SVM+XS)
- 第三方实例映像（如果已预配）

您必须将 NetScaler SDX 设备恢复到备份文件中可用的配置。在设备还原过程中，会删除整个当前配置。

如果要使用其他 NetScaler SDX 设备的备份还原 NetScaler SDX 设备，请确保在启动还原过程之前添加许可证并配置设备的管理服务网络设置以匹配备份文件中的设置。

确保已备份的 NetScaler SDX 平台变体与您尝试恢复的变体相同。不能从另一个平台变体还原。

> 注意：
>
> 在还原 SDX RMA 设备之前，请确保备份的版本与 RMA 版本相同或更高。

要从备份文件中恢复 SDX 装置，请执行以下操作：

1. 在 NetScaler 控制台 GUI 中，导航 到基础架构 **>** 实例 **> NetScaler**。
2. 点击 备份/还原。
3. 选择要恢复的同一个实例的备份文件。
4. 单击“重新打包备份”。

   备份 SDX 设备时，XVA 文件和图像将分开存储，以节省网络带宽和磁盘空间。因此，在恢复 SDX 设备之前，必须重新打包备份的文件。

   当您重新打包备份文件时，它会将所有备份文件包含在一起以恢复 SDX 设备。重新打包的备份文件可确保成功恢复 SDX 设备。
5. 选择重新打包的备份文件，然后单击“恢复”。

导出此控制板的报告

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

> 注意
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

强制故障转移到辅助 **NetScaler** 实例

January 29, 2024

例如，如果您需要更换或升级主 Citrix 应用程序 Delivery Controller (NetScaler) 实例，则可能需要强制进行故障转移。可以从主要实例或辅助实例强制执行故障转移。对主要实例强制执行故障转移时，主要实例变为辅助实例，而辅助实例变为主要实例。仅当主要实例可以确定辅助实例处于“UP”（运行）状态时才有可能执行强制故障转移。

强制故障转移不会传播，也不会同步。要在执行强制故障转移后查看同步状态，可以查看实例的状态。

在下列任何一种情况下，强制故障转移会失败：

- 在独立的系统上强制执行故障转移。
- 辅助实例处于禁用或非活动状态。如果辅助实例处于非活动状态，必须等待其状态变为“UP”（运行）时才能强制执行故障转移。
- 辅助实例配置为保持辅助状态。

如果 NetScaler 实例在您运行强制故障转移命令时检测到潜在问题，则会显示一条警告消息。该消息包括触发警告的信息，并在继续之前要求确认。

可以对主要实例或辅助实例强制执行故障转移。

要使用 **NetScaler** 控制台强制故障转移到辅助 **NetScaler** 实例，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例。转到 **VPX** 选项卡并选择一个实例。
2. 从所选实例类型下方列出的实例中选择 HA 设置中的实例。
3. 在“操作”框中，选择“强制故障转移”。
4. 单击 **Yes**（是）确认强制执行故障转移操作。

强制辅助 **NetScaler** 实例保持辅助状态

January 29, 2024

在高可用性 (HA) 设置中，无论主节点的状态如何，都可以强制辅助节点保持辅助节点。

例如，假定主节点需要升级，该过程需要数秒。升级期间，主节点可能会关闭几秒钟，但您不希望辅助节点接管，并且即使在主节点中检测到故障，也希望它仍然是辅助节点。

强制辅助节点保持辅助节点时，即使主节点关闭，它仍保持辅助节点。此外，如果强制使 HA 对中一个节点状态保持辅助状态，它将不会参与 HA 状态计算机转换。该节点的状态显示为 STAYSECONDARY。

> 注意
>
> 强制系统保持辅助状态时，强制过程不会传播或同步。它仅影响对其运行命令的节点。

要使用 **NetScaler** 控制台将辅助 **NetScaler** 实例配置为保持辅助状态，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 实例，然后在实例类型 (VPX) 下选择一个实例。
2. 从所选实例类型下方列出的实例中选择 HA 设置中的实例。
3. 在“操作”框中，选择“保持次要状态”。
4. 单击 是 以确认“保持次要”操作的执行。

创建实例组

January 29, 2024

要创建实例组，必须先将所有 NetScaler 实例添加到 NetScaler 控制台。成功添加实例后，根据实例系列创建实例组。创建一组实例可帮助您一次性对分组实例进行升级、备份或恢复。

使用 **NetScaler** 控制台创建实例组

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例 **>** 实例组，然后单击“添加”。
2. 为您的实例组指定一个名称，然后从“实 例系列”列 表中选择 **NetScaler** 。
3. 在 类别中，选择 默认 选项。
4. 单击 选择实例。在“选择实例”页面上，选择要分组的实例，然后单击“选择”。

   该表列出了所选实例及其详细信息。如果要从组中移除任何实例，请从表中选择该实例，然后单击“删除”。
5. 单击创建。

全局服务器负载平衡站点组

January 29, 2024

如果您想确保 ADC 实例的持续可用性和灾难恢复，可以配置 GSLB 站点组。它通过将客户端请求定向到最近或性能最佳的站点，或者在出现中断时引导到幸存的站点，来平衡站点间的负载。

有时，在 GSLB 站点组中，ADC 实例的配置对象会尝试相互覆盖。这会导致竞赛状态。要解决此类问题，您需要控制 GSLB 站点组中的主节点选择。主节点中的配置将应用于其余的 ADC 实例。在 NetScaler 控制台中，您可以创建 GSLB 站点组并执行以下操作：

- 在选定的 ADC 实例中选择一个主节点。
- 如果选定的主节点出现故障，请设置主节点选择的优先顺序。

您可以在 基础结构 **>** 实例 **> GSLB** 站点组中查看您的 **GSLB** 站点组。

创建 **GSLB** 站点组

执行以下步骤使用 ADC 实例创建 GSLB 站点组：

1. 转到 基础结构 **>** 实例 **> GSLB** 站点组。

2. 单击添加。
3. 指定 GSLB 站点组的名称。
4. 选择要在 GSLB 站点组中添加的实例。这些实例充当组中的站点。
5. 至少选择一个站点，然后单击“激活站点”。

   设置为优先级 1 的实例将成为主节点。您可以重新排序活跃站点的优先级。选择优先级较低的实例，然后单击 向上移动优先级。
6. 单击创建。

在 基础结构 **>** 网络功能 **> GSLB** 中，GUI 仅显示来自 GSLB 站点组主 ADC 节点的实体。

为 **NetScaler** 代理创建 **SNMP** 管理器和用户

January 29, 2024

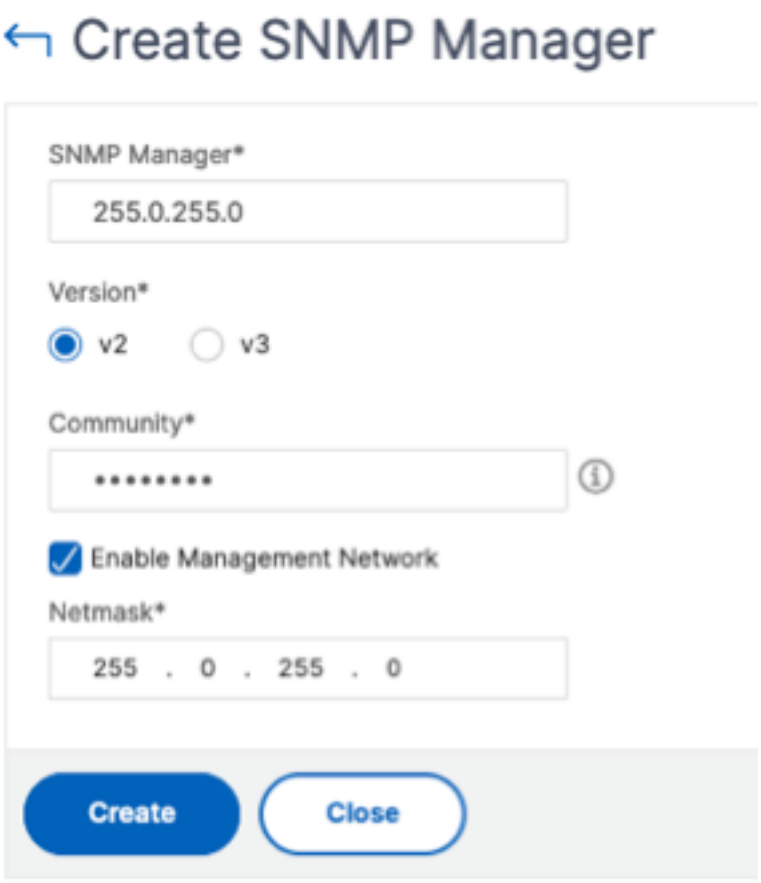
您可以从名为 SNMP 管理器的远程设备向 S NMP 代理查询系统特定信息。该代理随后会在管理信息库 (MIB) 搜索请求的数据，并将其发送到 SNMP 管理器。

您可以添加 SNMP 管理器来查询 NetScaler 代理。管理器符合 SNMP V2 和 V3 的要求。如果您指定一个或多个 SNMP 管理器，则 NetScaler 代理不接受来自除指定的 SNMP 管理器之外的任何主机的 SNMP 查询。

添加 **SNMP v2** 管理器

要为 NetScaler 代理添加 SNMP v2 管理器，请执行以下操作：

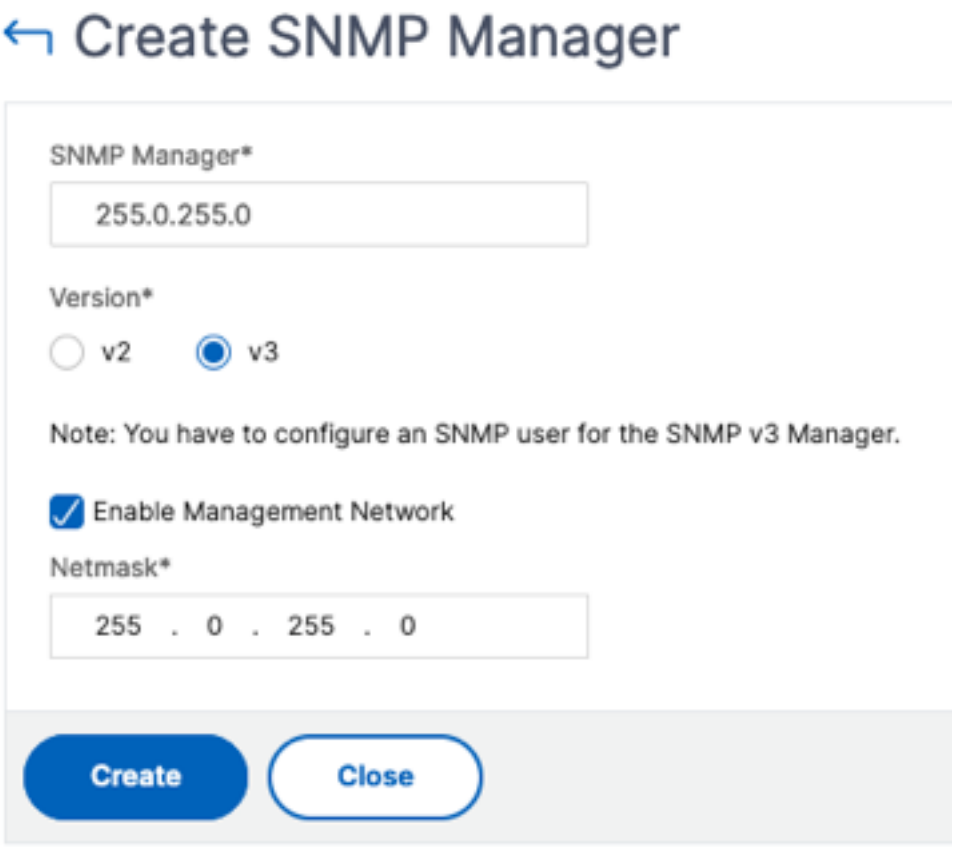
1. 导航到 基础架构 **>** 实例 **>** 代理，选择一个 NetScaler 代理，然后 单击选择操作 **>** 管理 **SNMP**。
2. 在“**SNMP**”**>**“**SNMP** 管理器”选项卡中，单击“添加”。
3. 在“创建 **SNMP** 管理器”页面中，指定以下详细信息：
   - **SNMP** 管理器。输入 SNMP 管理器的名称或 IP 地址。
   - 版本。选择 v2。
   - 社区。输入社区名称。SNMP 社区配置对来自 SNMP 管理器的 SNMP 查询进行身份验证。
   - 启用管理网络：选中此复选框可指定 SNMP 管理器网络的网络掩码。
   - 网络掩码：输入与 IP 地址关联的子网掩码。
4. 单击创建。



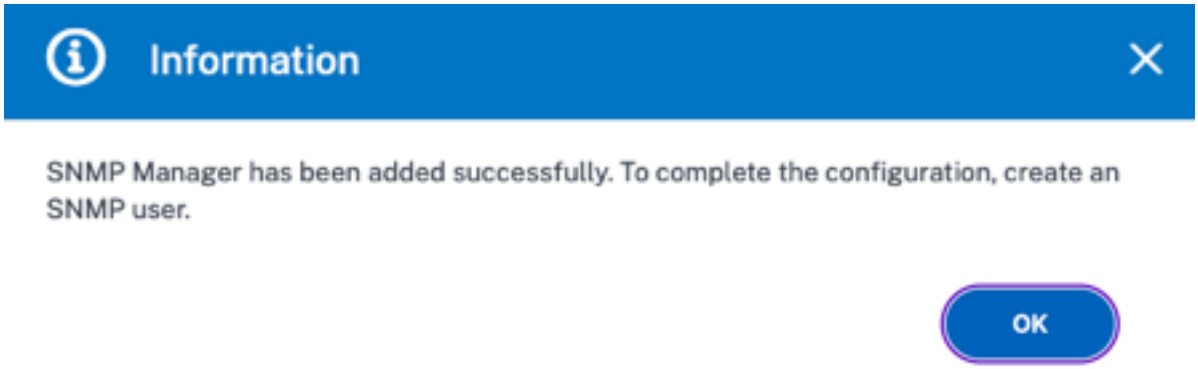
添加 **SNMP v3** 管理器

要为 NetScaler 代理添加 SNMP v3 管理器，请执行以下操作：

1. 导航到 基础架构 **>** 实例 **>** 代理，选择一个 NetScaler 代理，然后 单击“选择操作”**>**“管理 **SNMP**”。
2. 在“**SNMP**”**>**“**SNMP** 管理器”选项卡中，单击“添加”。
3. 在“创建 **SNMP** 管理器”页面中，指定以下详细信息：
   - **SNMP** 管理器。输入 SNMP 管理器的名称或 IP 地址。
   - 版本。选择 v3。
   - 启用管理网络：选中此复选框可指定 SNMP 管理器网络的网络掩码。
   - 网络掩码：输入与 IP 地址关联的子网掩码。
4. 单击创建。



出现一个对话框，确认已创建 SNMP 管理器并提示您配置 SNMP 用户。



> 注意：
>
> 必须为 SNMP v3 管理器配置 SNMP 用户。要配置 SNMP 用户，请转到 **SNMP > SNMP** 用户。

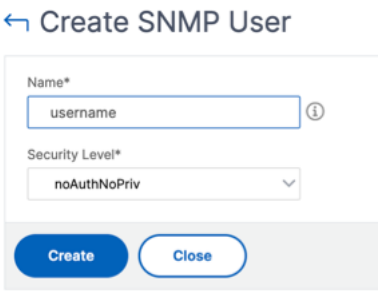
添加 **SNMP** 用户

添加一个 SNMP 用户来回应来自 SNMP 管理器的 SNMP v3 查询。

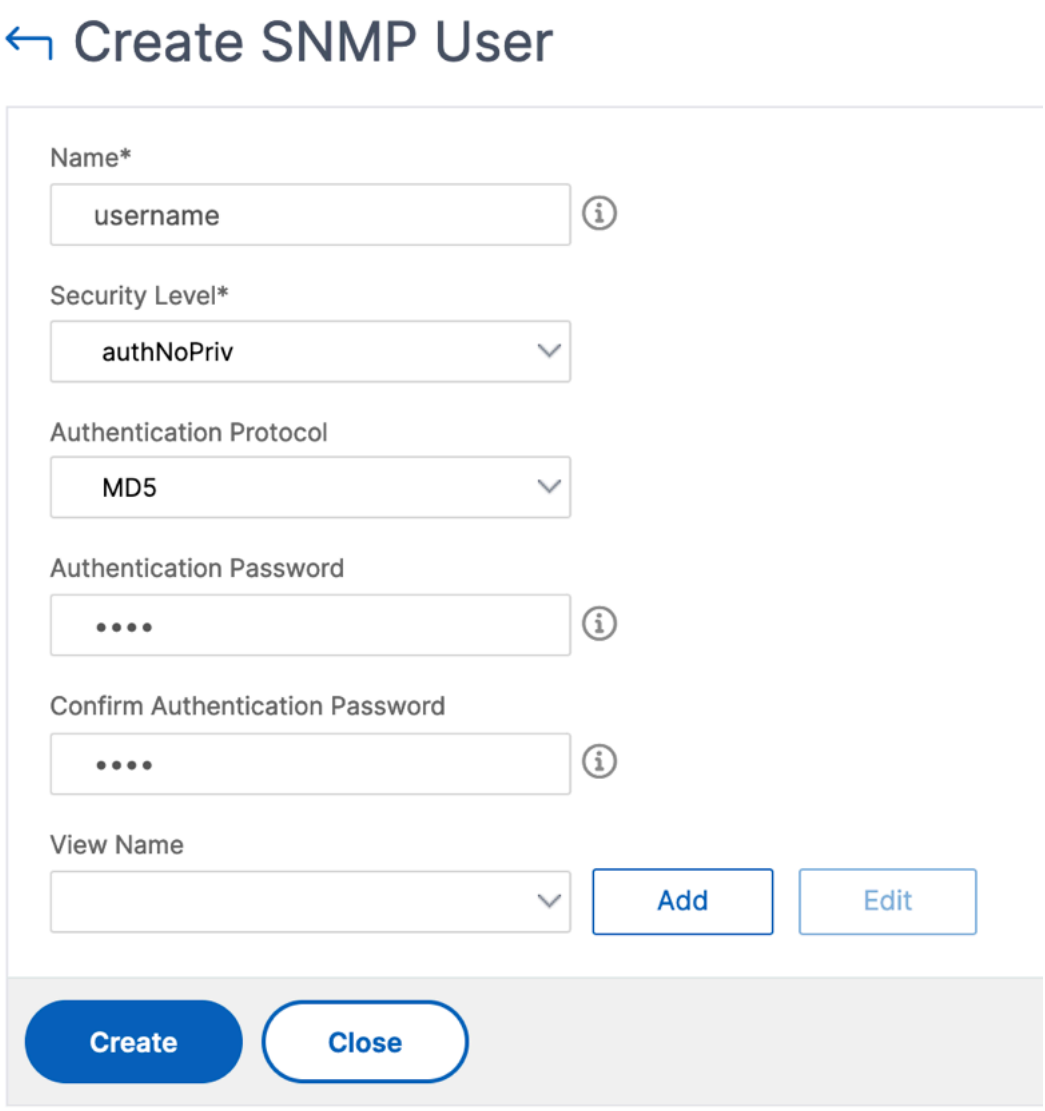
要为 NetScaler 代理添加 SNMP 用户，请执行以下操作：

1. 导航到 基础架构 **>** 实例 **>** 代理，选择一个 NetScaler 代理，然后 单击选择操作 **>** 管理 **SNMP**。
2. 在“**SNMP**”**>**“**SNMP** 用户”选项卡中，单击“添加”。
3. 在 创建 **SNMP** 用户 页面中，添加以下详细信息：
   - 名称。输入用户名。
   - 安全级别。NetScaler 代理与 SNMP 管理器之间通信所需的安全级别。

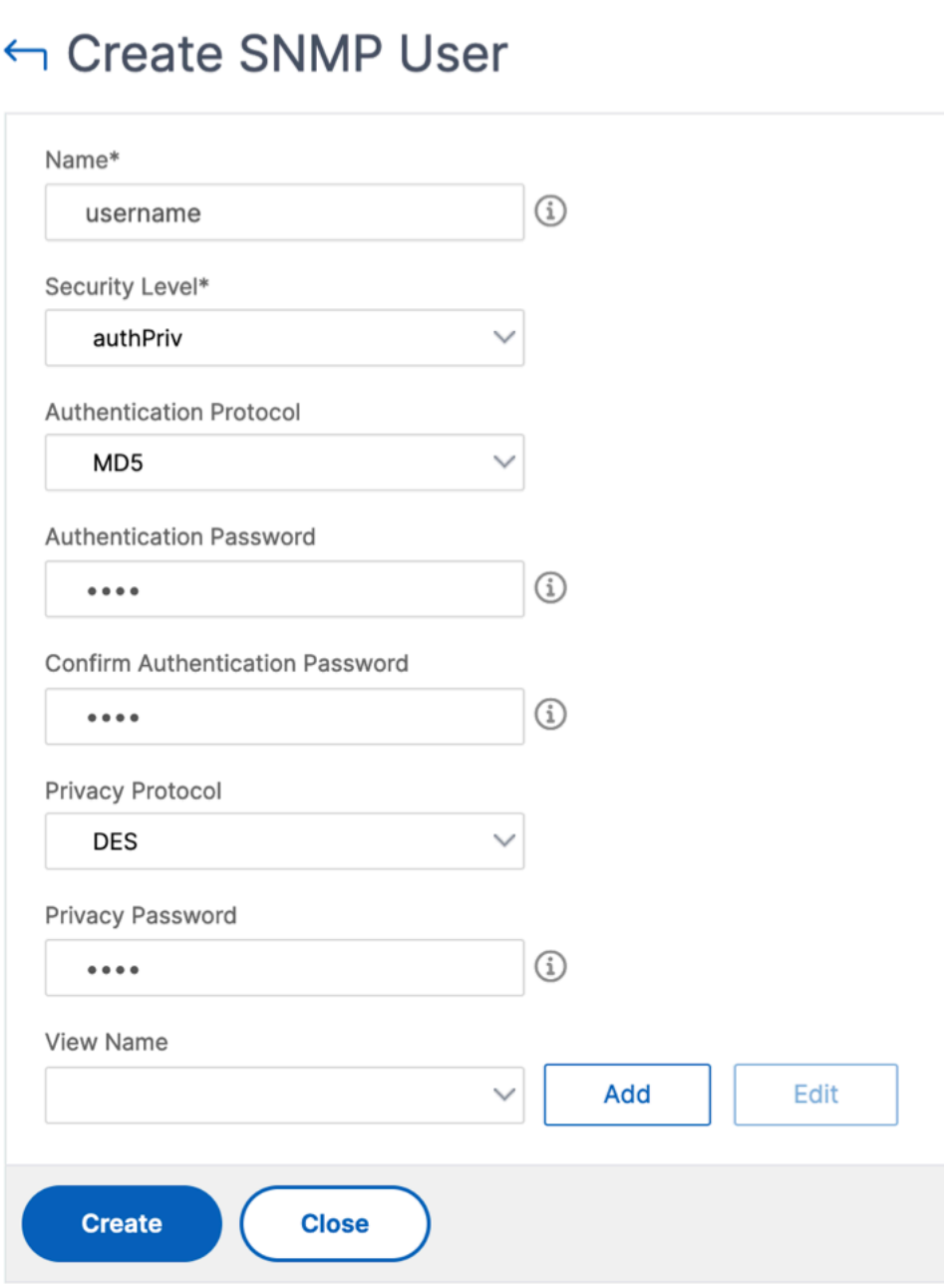
     选择以下安全级别之一：
   - **noAuthNoPriv**. 既不需要身份验证，也不需要加密。



   - **authNoPriv**. 需要身份验证但不需要加密。



- **authPriv**。需要身份验证和加密。



根据您分配给用户的安全级别，提供额外的身份验证协议，如身份验证协议、隐私密码和分配 SNMP 视图。

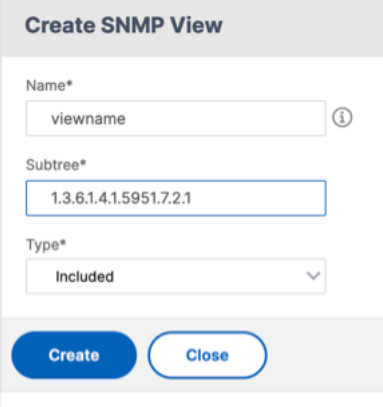
管理 **SNMP** 视图

SNMP 视图用于实现 SNMP 用户的访问控制。SNMP 视图限制用户访问 MIB 的特定部分。

要允许或限制 NetScaler 代理的 SNMP OID，请执行以下操作：

1. 导航到 基础架构 **>** 实例 **>** 代理，选择一个 NetScaler 代理，然后 单击“选择操作” **>** “管理 **SNMP**”。

2. 在“**SNMP**”>“**SNMP** 用户”选项卡中，单击“添加”。
3. 在 创建 **SNMP** 视图中，输入以下详细信息：
   - 视图名称：SNMP 视图的名称。一个实例可以有许多同名的 SNMP 视图，这些视图因素树参数设置而有所区别。
   - 子树：要与此 SNMP 视图关联的 MIB 树的特定分支（子树）。必须将子树指定为 SNMP OID。
   - 类型：此字段允许您在视图中包含或排除子树。
4. 单击创建。



在 **SDX** 上配置 **NetScaler VPX** 实例

January 29, 2024

您可以使用 NetScaler 控制台在 SDX 设备上预置一个或多个 NetScaler VPX 实例。您可以部署的实例数量取决于您购买的许可证。如果添加的实例数量等于许可中指定的数量，则 NetScaler 控制台不允许您预置更多 NetScaler 实例。

在开始之前，请确保在 NetScaler 控制台中添加一个 SDX 实例，用于配置 VPX 实例。

要配置 VPX 实例，请执行以下操作：

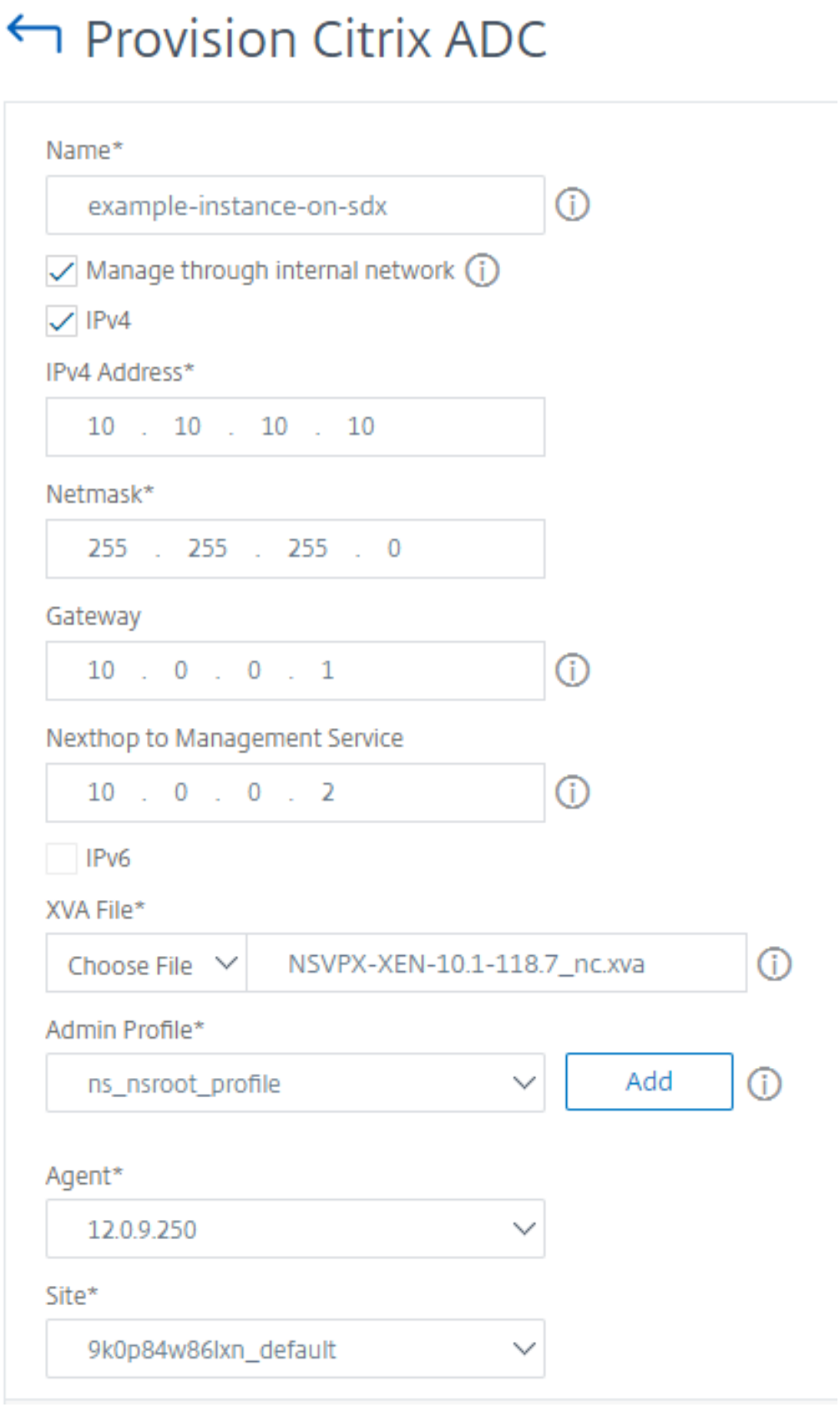
1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 在 **SDX** 选项卡中，选择要预配 VPX 实例的 SDX 实例。
3. 在 选择操作中，选择 预配 **VPX**。

步骤 **1-**添加 **VPX** 实例

NetScaler 控制台使用以下信息在 SDX 设备中配置 VPX 实例：

- 名称 - 指定 NetScaler 实例的名称。
- 在 SDX 和 VPX 之间建立通信网络。为此，请从列表中选择所需的选项：
  - 通过内部网络管理 -此选项为 NetScaler 控制台和 VPX 实例之间的通信建立内部网络。
  - **IP** 地址 -您可以选择 **IPv4** 或 **IPv6** 地址或同时选择两者来管理 NetScaler VPX 实例。VPX 实例只能有一个管理 IP（也称为 NetScaler IP）。您无法删除 NetScaler IP 地址。

    对于所选选项，为 IP 地址分配网络掩码、默认网关和 NetScaler 控制台的下一跳。
- **XVA** 文件 -选择要从中预配 VPX 实例的 XVA 文件。使用以下选项之一选择 XVA 文件。
  - 本地 -从本地计算机中选择 XVA 文件。
  - 设备-从 NetScaler 控制台文件浏览器中选择 XVA 文件。
- 管理员配置文 件-此配置文件提供对配置 VPX 实例的访使用此配置文件，NetScaler 控制台从实例检索配置数据。如果必须添加配置文件，请单击 添加。
- **Agent** -选择要与实例关联的代理
- 站点 -选择要添加实例的站点。



步骤 **2-**分配许可证

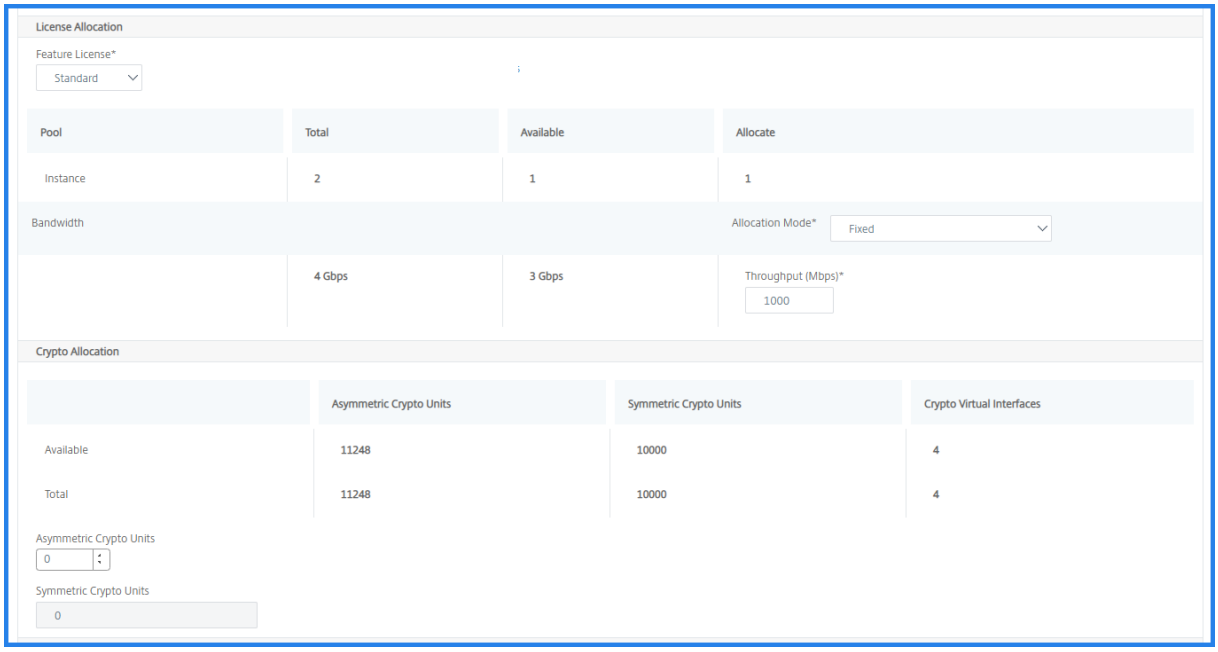
在“许可证分配”部分 中，指定 VPX 许可证。您可以使用标准、高级和高级许可证。

- 分配模式 -您可以为带宽池选择 固定或突发 模式。

  如果选择 突发模式，则可以在达到固定 带宽时使用额外的带宽。

- 吞吐量 -将总吞吐量（以 Mbps 为单位）分配给实例。

> 注意
>
> 为 SDX 设备上的 Citrix Secure Web Gateway (SWG) 实例单独购买许可证（用于安全 Web Gateway 的 SDX 2 实例附加包）。此实例包不同于 SDX 平台许可证或 SDX 实例包。
>
> 有关更多信息，请参阅 在 SDX 设备上部署 Citrix Secure Web Gateway 实例。



从 SDX 12.0 57.19 版本开始，管理加密容量的界面发生了变化。有关更多信息，请参阅 管理加密容量。

步骤 **3-**分配资源

在“资源分配”部分 中，将资源分配给 VPX 实例以维护流量。

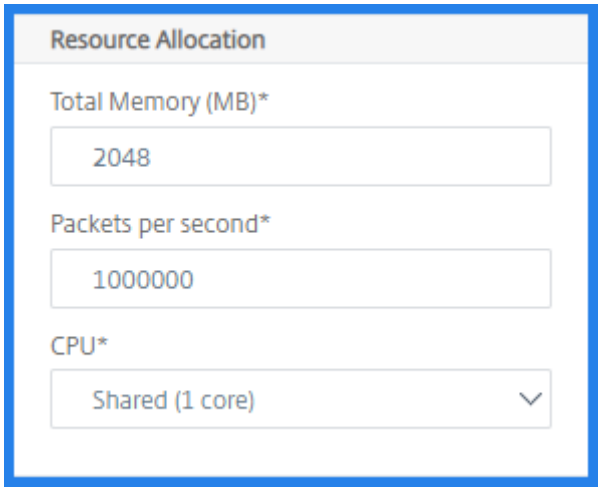
- 总内存 **(MB)** -为实例分配总内存。最小值为 2048 MB。
- 每秒数据包 数-指定每秒要传输的数据包数。
- **CPU** -指定实例的 CPU 内核数。您可以使用共享或专用 CPU 内核。

  当您为实例选择共享内核时，其他实例可以在资源短缺时使用共享内核。

重新启动重新分配 CPU 核心的实例，以避免任何性能下降。

如果您使用的是 SDX 25000xx 平台，则最多可以为实例分配 16 个内核。此外，如果您使用的是 SDX 2500xxx 平台，则最多可以为实例分配 11 个内核。

> 注意
>
> 对于实例，您配置的最大吞吐量为 180 Gbps。



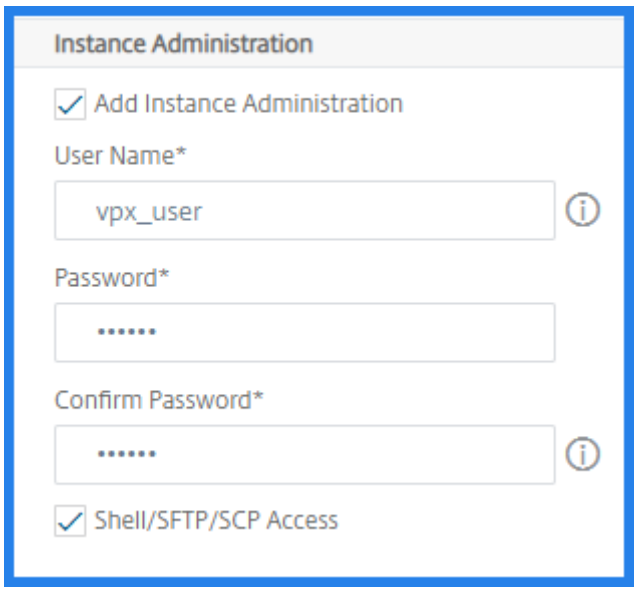
请参阅 Prov ision NetScaler 实例 中的表格，其中列出了支持的 VPX、单包映像版本以及可以分配给实例的内核数量。

步骤 **4-**添加实例管理

您可以为 VPX 实例创建管理员用户。为此，请在“实例管理”部分中选择添加实例管理。

指定以下详细信息：

- 用户名：NetScaler 实例管理员的用户名。此用户具有超级用户访问权限，但无权访问联网命令来配置 VLAN 和接口。
- 密码：指定用户名的密码。
- **Shell/Sftp/Scp** 访问权限：允许给 NetScaler 实例管理员的访问权限。此选项默认处于选中状态。



步骤 **5-**指定网络设置

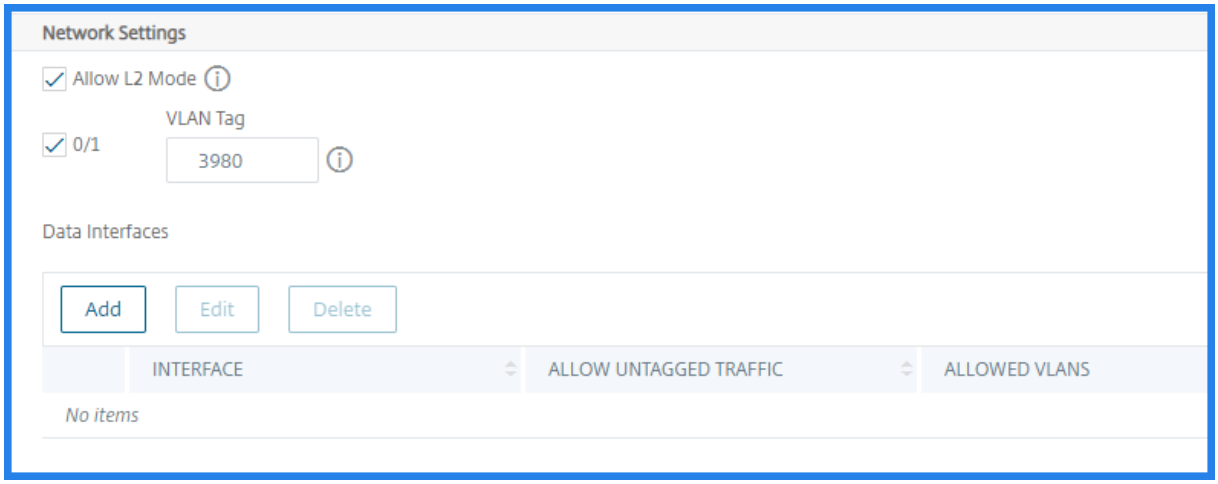
为实例选择所需的网络设置：

- 在网络设置下允许 **L2** 模式 -您可以在 NetScaler 实例上允许 L2 模式。在“网络设置”下选择“允许 L2 模式”。在登录实例并启用 L2 模式之前。有关更多信息，请参阅在 NetScaler 实例上允许 L2 模式。

  > 注意：
  >
  > 如果您为实例禁用 L2 模式，则必须登录该实例并从该实例禁用 L2 模式。否则，它可能会导致在重新启动实例后所有其他 NetScaler 模式被禁用。

- **0/1** -在 **VLAN** 标记中，为管理接口指定 VLAN ID。
- **0/2** -在 **VLAN** 标记中，为管理接口指定 VLAN ID。

默认情况下，接口 **0/1** 和 **0/2** 处于选中状态。

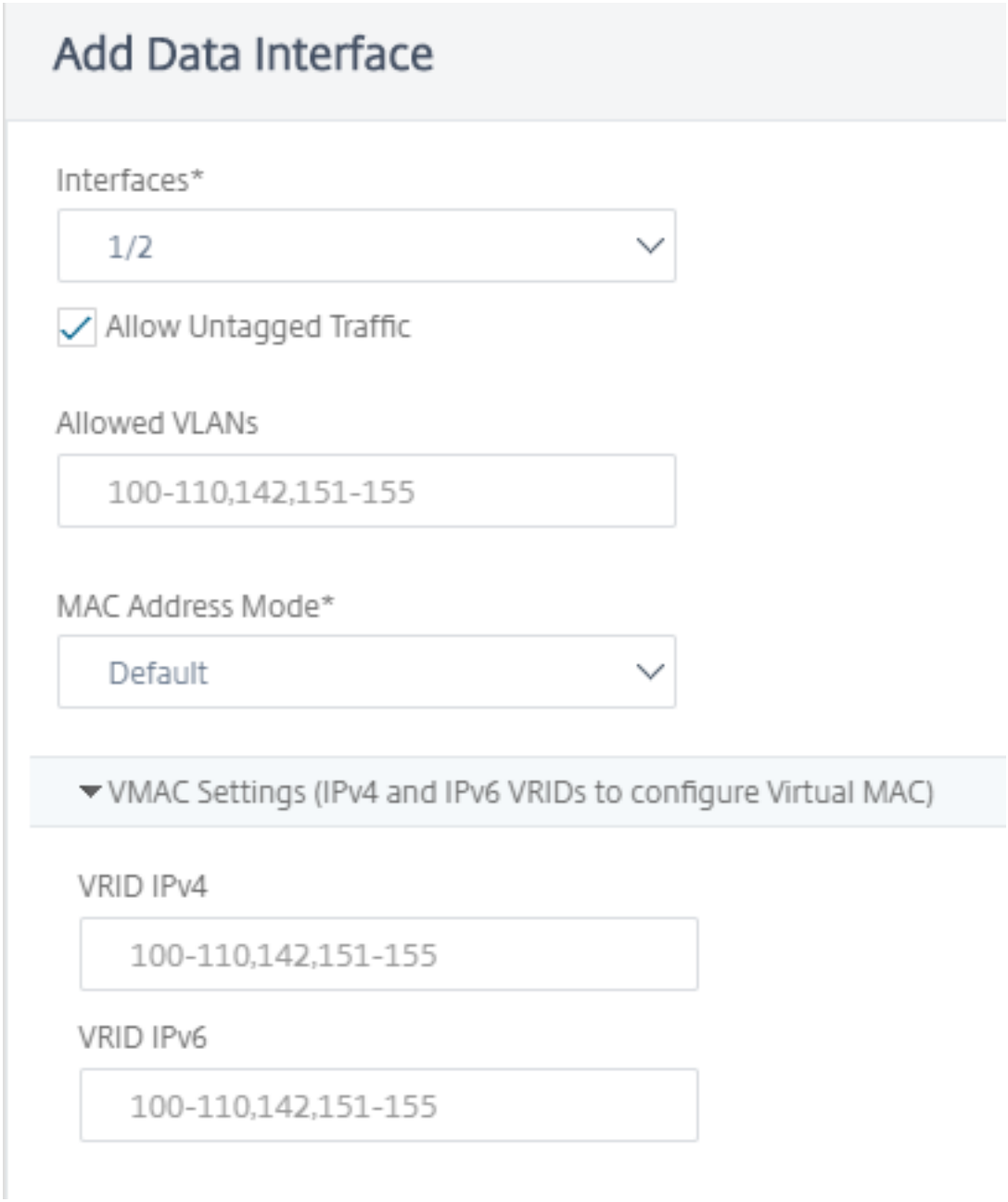


在 数据接口中，单击 添加 以添加数据接口并指定以下内容：

- 接口 -从列表中选择接口。

  > 注意：
  >
  > 添加到实例的接口的接口 ID 不一定与 SDX 设备上的物理接口 ID 相对应。
  >
  > 例如，与实例 1 关联的第一个接口是 SDX 接口 1/4，当您查看该实例中的接口设置时，它显示为接口 1/1。此接口表示它是您与 instance-1 关联的第一个接口。

- 允许的 **VLAN** -指定可与 NetScaler 实例关联的 VLAN ID 列表。
- **MAC** 地址模式 -为实例分配 MAC 地址。选择以下选项之一：
  - 默认 -Citrix Workspace 分配 MAC 地址。
  - 自定义 -选择此模式可指定覆盖生成的 MAC 地址的 MAC 地址。
  - 已生 成-使用之前设置的基本 MAC 地址生成 MAC 地址。有关设置基本 MAC 地址的信息，请参阅 为接口分配 MAC 地址。
- **VMAC** 设置（用于配置虚拟 **MAC** 的 **IPv4** 和 **IPv6 VRID**）
  - **VRID IPV4** -标识 VMAC 的 IPv4 VRID。可能的值：1—255。有关更多信息，请参阅在接口上配置 VMAC。
  - VRID IPv6 - 标识 VMAC 的 IPv6 VRID。可能的值：1—255。有关更多信息，请参阅在接口上配置 VMAC。



单击添加。

步骤 **6-**指定管理 **VLAN** 设置

VPX 实例的管理服务和管理地址 (NSIP) 位于同一子网中，通信通过管理接口进行。

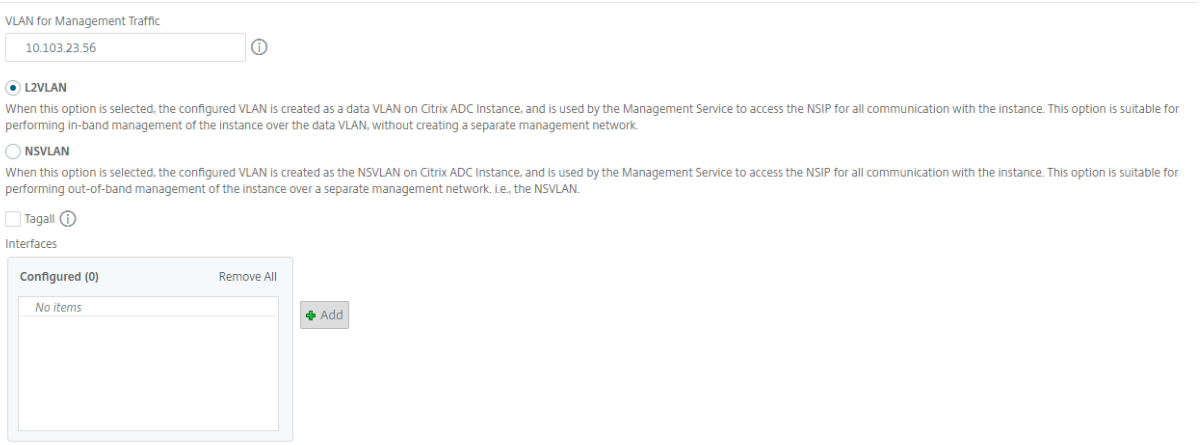
如果管理服务和实例位于不同的子网中，请在配置 VPX 实例时指定 VLAN ID。因此，当实例处于活动状态时，可通过网络访问该实例。

如果您的部署要求 NSIP 只能在配置 VPX 实例时通过选定的接口访问，请选择 **NSVLAN**。而且，NSIP 变得无法通过

其他接口访问。

- HA 检测信号仅在属于 NSVLAN 的接口上发送。
- 只能从 VPX XVA 内部版本 9.3-53.4 及更高版本中配置 NSVLAN。

> 重要
>
> - 预配 VPX 实例后，您无法更改此设置。
> - 如果未选择 **NSVLAN**，**VPX** 实例上的 **`clear config full`** 命令将删除 **VLAN** 配置。

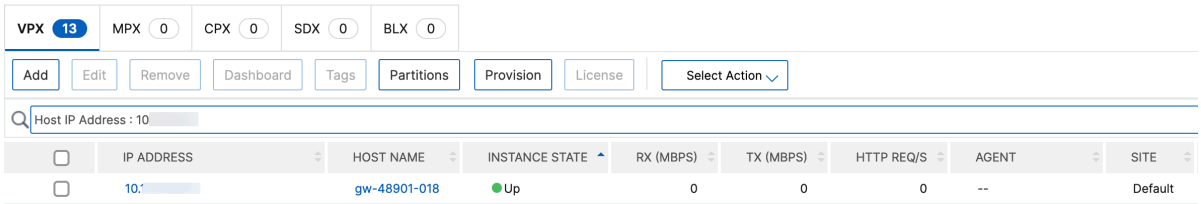


单击“完成”以配置 VPX 实例。

查看预配置的 **VPX** 实例

要查看新配置的实例，请执行以下操作：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 在 **VPX** 选项卡中，按 主机 **IP** 地址 属性搜索实例，然后为其指定 SDX 实例 IP。



重新发现多个 **NetScaler** 实例

January 29, 2024

您可以在 NetScaler 控制台设置中重新发现多个 Citrix Application Delivery Controller (NetScaler) 实例（VPX、MPX、SDX、BLX 和 CPX）。重新发现实例后，您可以查看这些实例的最新状态和配置。NetScaler 控制台服务器会重新发现所有 ADC 实例并检查这些实例是否可访问。

要重新发现多个 **NetScaler VPX** 实例，请：

1. 导航到基础结构 **>** 实例 **> NetScaler**。选择实例选项卡（VPX、MPX、SDX、BLX 和 CPX），然后选择要重新发现的实例。
2. 在 操 作框中，单击 重新发现。您还可以重新发现多个 VPX 实例。
3. 当显示运行“重新发现”实用程序的确认消息时，单击 是”。

   屏幕报告每个实例的重新发现进度。

轮询概述

January 29, 2024

轮询是一个过程，在这个过程中，NetScaler 控制台从 NetScaler 实例收集某些信息。您可能已在全球范围内为您的组织配置了多个 NetScaler 实例。要通过 NetScaler 控制台监视您的实例，NetScaler 控制台必须收集某些信息，例如 CPU 使用率、内存使用情况、SSL 证书、许可功能、所有托管 NetScaler 实例的许可类型。以下是 NetScaler 控制台和托管实例之间发生的不同类型的轮询：

- 实例轮询
- 清单轮询
- 性能数据收集
- 实例备份轮询
- 配置审核投票
- SSL 证书轮询
- 实体轮询

NetScaler 控制台使用 NITRO 调用、安全外壳 (SSH) 和安全复制 (SCP) 等协议来轮询来自 NetScaler 实例的信息。

NetScaler 控制台如何轮询托管实例和实体

默认情况下，NetScaler 控制台会自动定期轮询。NetScaler 控制台还允许您为几种轮询类型配置轮询间隔，并允许您在需要时手动轮询。

下表描述了轮询类型、轮询间隔、使用的协议等的详细信息：

轮询类型	轮询时间间隔	民意调查信息	使用的协议	轮询间隔配置
实例轮询	每 5 分钟（默认）	统计信息，例如状态、每秒 HTTP 请求数、CPU 使用率、内存使用率和吞吐量。	NITRO call。	否
清单轮询	每 60 分钟（默认）	清单详细信息，如构建版本、系统信息、许可功能和模式。	NITRO 通话和 SSH	否
性能数据收集	每 5 分钟（默认）	网络报告信息	NITRO call	否
实例备份轮询	每 12 小时（默认情况下）	托管 NetScaler 实例当前状态的备份文件	NITRO 调用、SSH 和 SCP。	是。导航到基础结构 **>** 实例 **>** **NetScaler**。选择实例，然后从 选择操作”列表中单击“备份/还原。
配置审核投票	每 10 小时（默认情况下）	在 NetScaler 实例上发生的配置更改（例如，运行配置与保存的配置）	SSH、SCP 和 NITRO 通话	是。导航到 基础结构 **>** 配置 **>** 配置审核。在“配置审核”页上，单击 设置 并配置配置审核轮询的轮询间隔。 您可以手动轮询配置审核，并将实例的所有配置审核立即添加到 NetScaler 控制台。为此，请导航到基础结构 **>** 配置 **>** 配置审核，然后单击 立即轮询。立即投票 页面允许您轮询网络中的所有实例或选定实例。
SSL 证书轮询	每 24 小时一次（默认）	安装在 NetScaler 实例上的 SSL 证书。	NITRO 电话和 SCP	是。导航到 基础结构 **> SSL** 控制面板。在“SSL 控制面板”页上，单击 设置 以配置轮询间隔

轮询类型	轮询时间间隔	民意调查信息	使用的协议	轮询间隔配置
实体轮询	每 60 分钟（默认）	在实例上配置的所有实体。实体是附加到 NetScaler 实例的策略、虚拟服务器、服务或操作。要启用实体轮询，请参见 启用或禁用 NetScaler 控制台功能。	NITRO 调用。	您可以手动轮询 SSL 证书，并将实例的所有证书立即添加到 NetScaler 控制台。为此，请导航到 基础结构 **> SSL** 控制面板，然后单击 立即轮询。立即投票 页面允许您轮询网络中的所有实例或选定实例。可以，但不能设置为少于 10 分钟。要进行配置，请导航到 基础结构 **>** 网络功能。在“网络功能”页上，单击 设置 以配置轮询间隔。 您可以手动轮询实体，并将实例的所有实体立即添加到 NetScaler 控制台。为此，请导航到 基础结构 **>** 网络功能，然后单击 立即轮询。立即轮询 页面允许您轮询网络中的所有实例或选定的实例

> 注
>
> 意：除轮询外，NetScaler 托管实例生成的事件还通过发送到实例的 SNMP 陷阱由 NetScaler 控制台接收。例如，系统发生故障或配置发生更改时生成事件。
>
> 在实例备份期间，SSL 文件、CA 证书文件、NetScaler 模板、数据库信息等会下载到 NetScaler 控制台。在配置审核过程中，ns.conf 文件会下载并存储在文件系统中。从托管 NetScaler 实例收集的所有信息都存储在数据库内部。

轮询实例的不同方式

以下是 NetScaler 控制台在托管实例上执行的不同轮询方式：

- 对实例进行全局轮询
- 手动轮询实例
- 对实体进行人工投票

对实例进行全局轮询

NetScaler 控制台根据您配置的时间间隔自动轮询网络中的所有托管实例。尽管默认轮询间隔为 60 分钟，但您可以通过导航到 基础结构 **>** 网络功能 **>** 设置来根据需要设置间隔。

手动轮询实例

当 NetScaler 控制台管理多个实体时，轮询周期会花费更长的时间来生成报告，这可能会导致屏幕空白，或者系统可能仍显示之前的数据。

在 NetScaler 控制台中，不进行自动轮询时有一个最短的轮询间隔周期。如果您添加新的 NetScaler 实例，或者更新了实体，NetScaler 控制台在下次轮询之前无法识别新实例或对实体所做的更新。并且，没有办法立即获取虚拟 IP 地址列表来执行进一步操作。您必须等待最小轮询时间间隔过去。尽管您可以通过手动轮询来发现新添加的实例，但这会导致对整个 NetScaler 网络进行轮询，从而给网络带来沉重的负载。现在，NetScaler 控制台不允许您在任何给定时间轮询选定的实例和实体，而非轮询整个网络。

NetScaler 控制台会自动轮询托管实例，以在一天中的设定时间收集信息。选定轮询缩短了 NetScaler 控制台显示绑定到这些选定实例的实体的最新状态所需的刷新时间。

要在 **NetScaler** 控制台中轮询特定实例，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 网络功能。
2. 在 网络功能 页上的右上角，单击 立即轮询。
3. 弹出页面“立即轮询”为您提供了轮询网络中所有 NetScaler 实例或轮询选定实例的选项。
    a) “所有实例”选项卡-单击“开始轮询”以轮询 所有实例。
    b) 选择实例 选项卡-从列表中选择实例
4. 单击 开始轮询。

    NetScaler 控制台启动手动轮询并添加所有实体。

对实体进行人工投票

NetScaler 控制台还允许您仅轮询绑定到实例的少数选定实体。例如，您可以使用此选项来了解实例中特定实体的最新状态。在这种情况下，您无需轮询整个实例即可了解已更新实体的状态。当您选择和轮询一个实体时，NetScaler 控制台仅轮询该实体并在 NetScaler 控制台 GUI 中更新状态。

以虚拟服务器处于 关闭状态的示例为例。在下一次自动轮询发生之前，该虚拟服务器的状态可能已更改为 **UP**。要查看虚拟服务器的更改状态，您可能只想轮询该虚拟服务器，以便在 GUI 上立即显示正确的状态。

现在，您可以轮询以下实体的状态、服务、服务组、负载平衡虚拟服务器、缓存减少虚拟服务器、内容交换虚拟服务器、身份验证虚拟服务器、VPN 虚拟服务器、GSLB 虚拟服务器和应用程序服务器中的任何更新。

> 注意：
>
> 如果您轮询虚拟服务器，则只轮询该虚拟服务器。服务、服务组和服务器等相关实体不进行轮询。如果您需要轮询所有关联实体，则必须手动轮询这些实体，或者必须轮询实例。

要在 **NetScaler** 控制台中轮询特定实体，请执行以下操作：

例如，此任务可帮助您轮询负载平衡虚拟服务器。同样，您也可以轮询其他网络函数实体。

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 网络功能 **>** 负载平衡 **>** 虚拟服务器。
2. 选择状态显示为“关闭”的虚拟服务器，然后单击“立即轮询”。虚拟服务器的状态现在更改为 **UP**。

取消托管实例

January 29, 2024

如果您想停止 NetScaler 控制台与网络中的实例之间的信息交换，则可以取消对实例的管理。

要取消管理实例，请执行以下操作：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 选择 NetScaler 实例选项卡（例如，VPX）。
3. 在实例列表中，右键单击实例，然后选择取 消管理，或者选择实例，然后从 操作列表中选择取 消管理。

   所选实例的状态更改为“不服务”。

   该实例不再由 NetScaler 控制台管理，也不再与 NetScaler 控制台交换数据。

跟踪到实例的路由

January 29, 2024

通过跟踪数据包从 NetScaler 控制台到实例的路由，您可以找到诸如到达该实例所需的跳数之类的信息。traceroute 跟踪数据包从源到目的地的路径。它显示网络跃点列表以及路由中每个实体的主机名和 IP 地址。

Traceroute 也记录数据包从一个跃点传输到另一个跃点所用时间。如果数据包的传输有任何中断，traceroute 将显示问题存在的位置。

要跟踪实例的路由，请执行以下操作：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 选择 NetScaler 实例选项卡（例如，VPX）。
3. 在实例列表中，右键单击某个实例，然后选择 **Traceroute**，或者选择该实例，然后从操作列表中单击 **Traceroute**。

   “TraceRoute”（路由跟踪）消息框将显示实例的路由以及每个跃点所用时间（以毫秒为单位）。

查看 **NetScaler** 拥有的 **IP** 地址

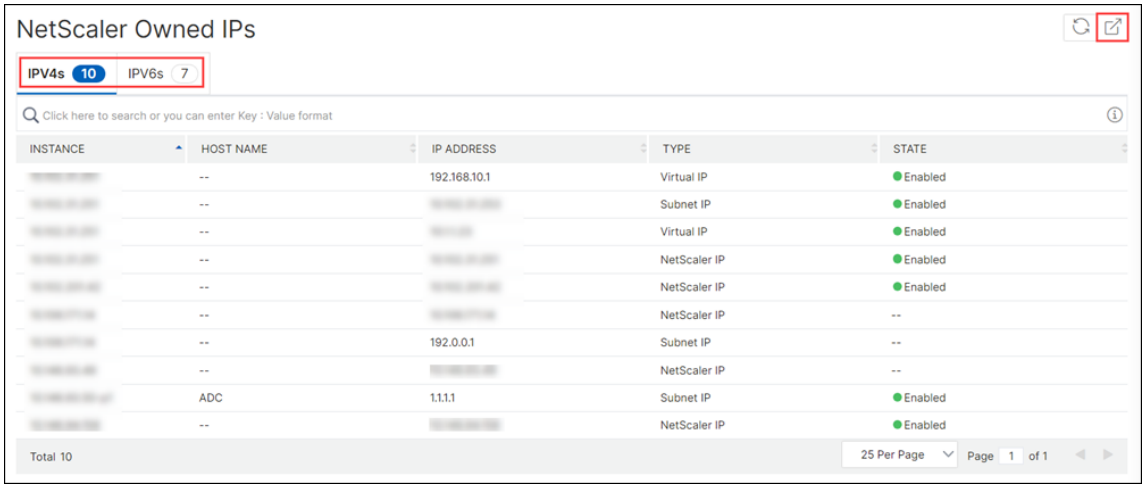
July 17, 2024

您可以直接从 NetScaler 控制台 GUI 中查看在 NetScaler 实例上配置的 IP 地址。请注意，配置更改和其他操作只能在 NetScaler 实例上执行。

要查看 NetScaler 拥有的 IP 地址，请导航到基础结构 **>** 实例 **> NetScaler** 拥有的 **IP**。

此功能显示在 NetScaler 实例上配置的 IPv4 和 IPv6 地址。IP 地址的类型包括：

- NetScaler IP 地址
- 子网 IP 地址
- 虚拟 IP 地址
- ADNS 服务 IP 地址
- GSLB IP 地址
- 群集 IP 地址
- 映射的 IP 地址



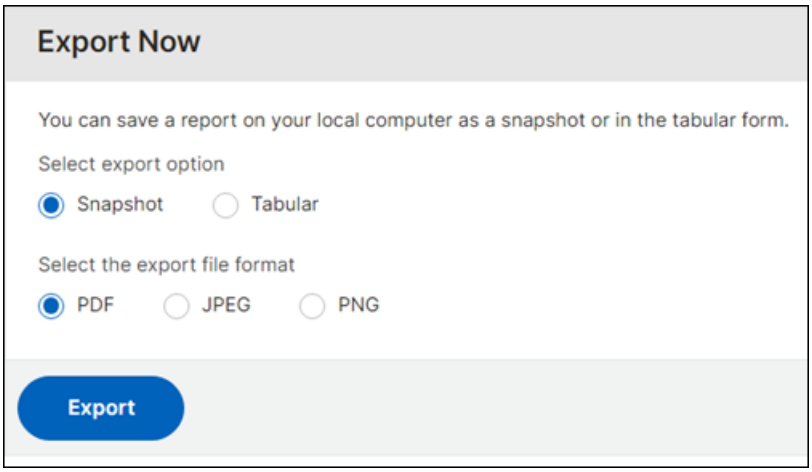
导出 **NetScaler** 拥有的 **IP** 地址

要导出 NetScaler 拥有的 IP 地址，请执行以下步骤：

1. 导航到基础结构 **>** 实例 **> NetScaler** 拥有的 **IP**。
2. 在 **NetScaler** 拥有的 **IP** 页面上，单击右上角的导出图标。
3. 在“导出报告”页面上，单击“立即导出”。
4. 在“立即导出”页面上，选择导出选项：

   对于快照导出：

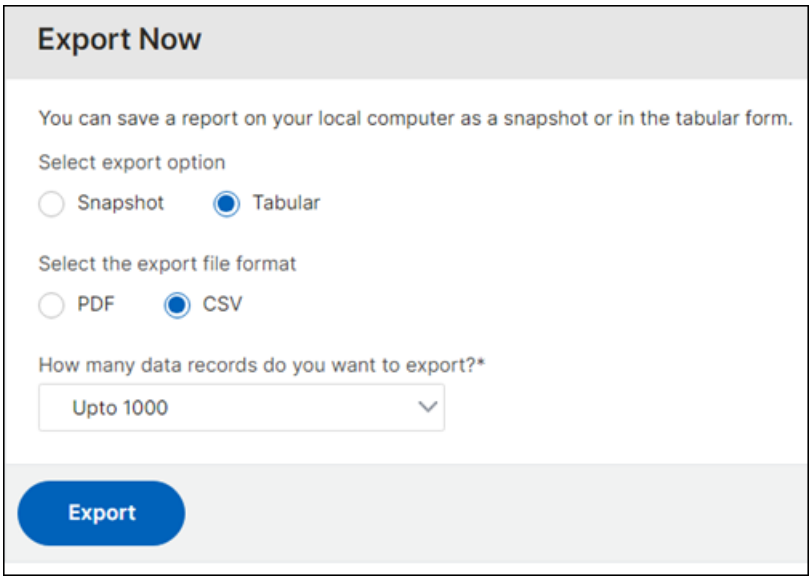
   a) 选择导出文件格式：PDF、JPG 或 PNG。



   对于表格导出：

   a) 选择导出文件格式：PDF 或 CSV。

b) 从列表中选择要导出的数据记录的数量。



5. 单击导出。

安排 **NetScaler** 拥有的 **IP** 地址的导出

要计划导出 NetScaler 拥有的 IP 地址，请执行以下步骤：

1. 导航到基础结构 **>** 实例 **> NetScaler** 拥有的 **IP**。
2. 在 **NetScaler** 拥有的 **IP** 页面上，单击右上角的导出图标。
3. 在“导出报告”页面上，单击“计划导出”。
4. 在“计划导出”页面上，输入以下详细信息：

   a) 输入主题和描述。

   b) 选择导出类型。

   对于快照导出类型：

   - 选择导出文件格式：PDF、JPG 或 PNG。

   对于表格导出类型：

   - 选择导出文件格式：PDF 或 CSV。
   - 从列表中选择要导出的数据记录的数量。

   c) 选择重复周期：每天、每周或每月。

   d) 选择导出时间。

e) 选择如何发送导出的 IP 地址：电子邮件、Slack 或两者兼而有之。

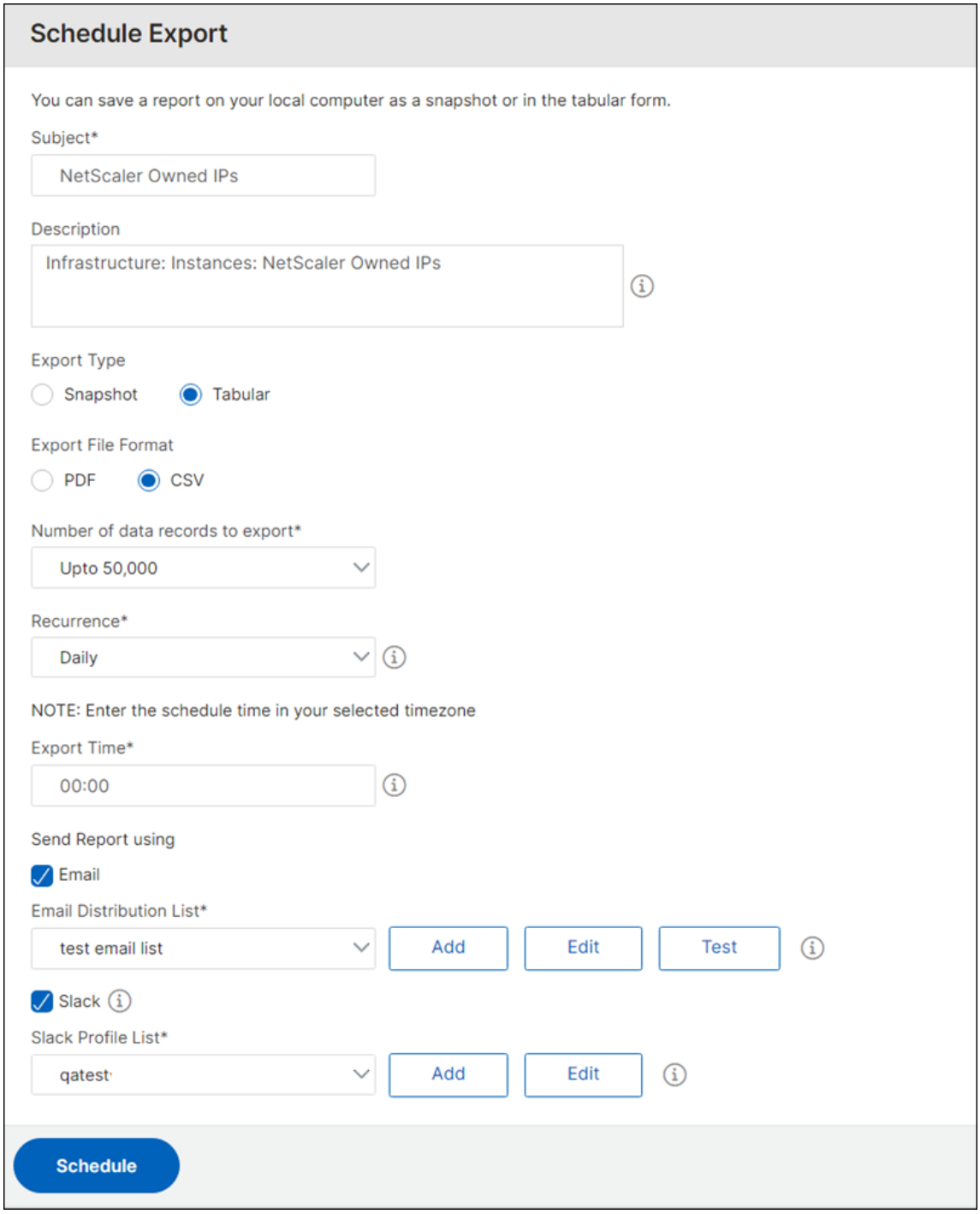
对于电子邮件：

- 选择电子邮件，然后选择电子邮件分发列表以发送 NetScaler 拥有的 IP 地址列表。
  - 要添加电子邮件分发列表，请单击“添加”并指定电子邮件服务器的详细信息。
  - 要编辑电子邮件分发列表，请单击“编辑”。
  - 要验证电子邮件分发列表是否正常运行，请单击“测试”。这将向选定的电子邮件分发列表发送一封测试电子邮件。

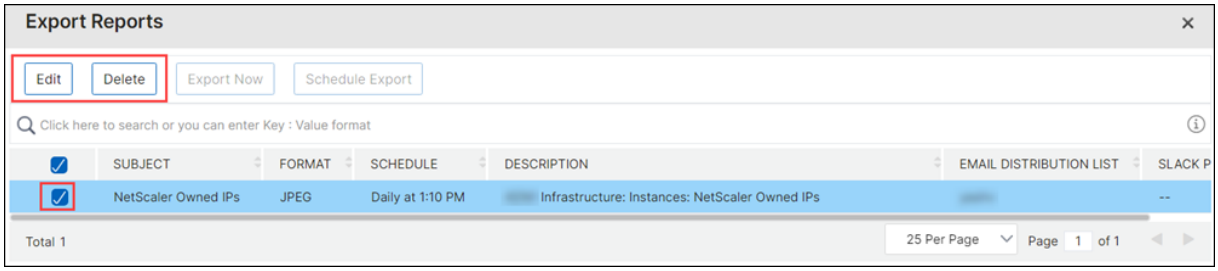
对于 Slack：

- 选择 **Slack** 并选择 Slack 配置文件列表以发送 NetScaler 拥有的 IP 地址列表。
  - 要添加 Slack 配置文件，请单击“添加”并指定 Slack 频道的配置文件名称、频道名称和令牌。
  - 要编辑现有 Slack 频道，请单击“编辑”。

5. 单击“计划”来安排导出。



计划完成后，您的导出计划将显示在“导出报告”页面上，您可以选择计划来执行编辑或删除操作。



如何更改 **NetScaler MPX** 或 **VPX** 根密码

January 29, 2024

有时，出于安全原因或密码轮换策略的合规性，您必须更改 NetScaler 设备的根密码。

本文档描述了更改通过 NetScaler 控制台云管理的 NetScaler MPX 和 VPX 设备的根密码所需的步骤。

如果您更改 NetScaler 密码，则必须修改与 NetScaler 关联的 NetScaler 控制台管理配置文件。NetScaler 控制台管理配置文件维护 NetScaler 凭据，用于与 NetScaler 设备进行基于 REST API、SSH、SCP 或 SNMP 的通信。通过管理配置文件，NetScaler 控制台管理 NetScaler MPX 和 VPX 设备。

使用 配置作业 功能更改密码

通过使用 NetScaler 控制台配置任务功能，您可以简化重复的密码更改过程，并将更改应用到 NetScaler 设备，而无需访问单个实例。

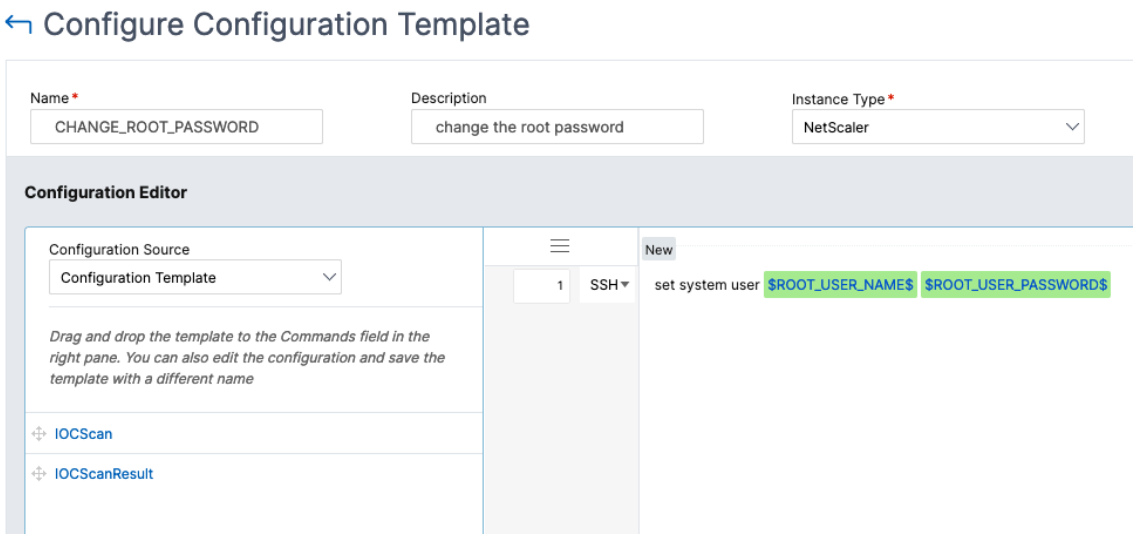
请按照以下步骤更改密码：

- 步骤 1. 创建配置模板。
- 步骤 2. 创建配置作业。
- 步骤 3. 创建管理员配置文件并对其进行修改。

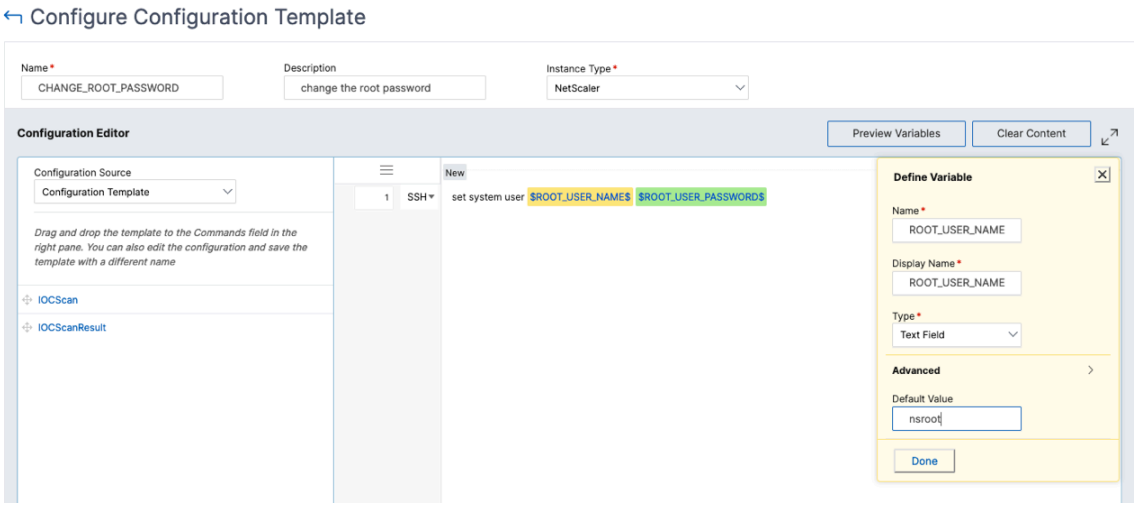
> 注意：
>
> 如果 NetScaler 设备也由其他工具管理，则还必须更改这些工具的证书。

创建 配置模板

1. 在 NetScaler 控制台 GUI 中，导航到基础架构 **>** 配置作业 **>** 配置模板。
2. 选择添加。通过键入 SSH 命令创建配置模板`set system user $ROOT_USER_NAME$ $ROOT_USER_PASSWORD$`。



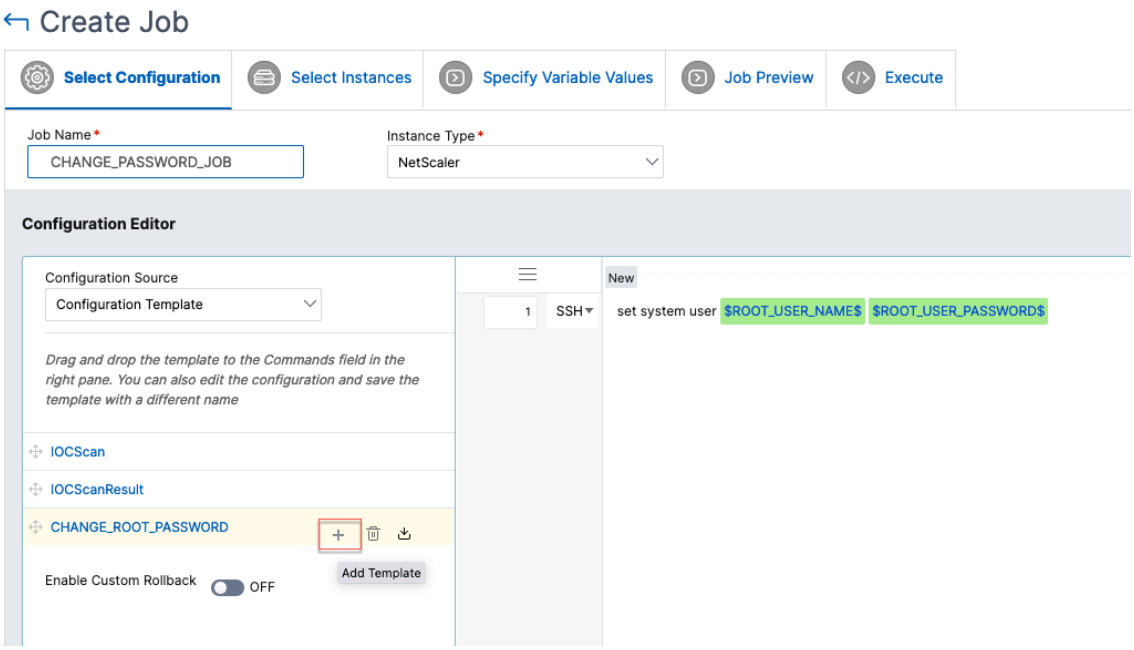
3. 选择 $ROOT_USER_NAME$ 变量，然后选择文本字段作为类型。
4. 或者，提供 root 用户名的默认值。选择 完成 以保存变量设置。



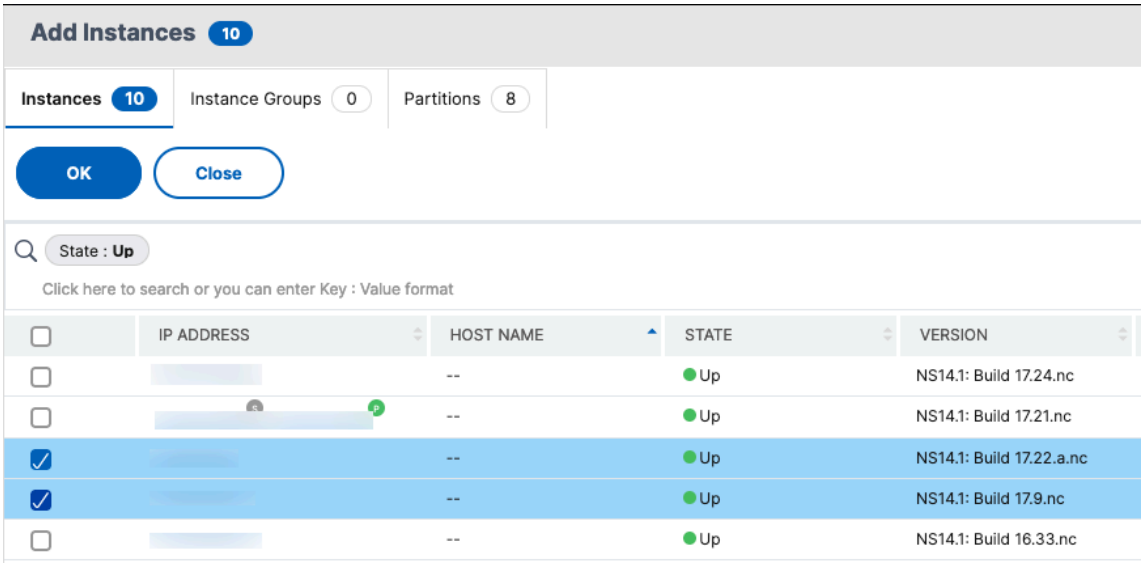
5. 选择 $ROOT_USER_PASSWORD$ 变量，然后选择密码字段作为类型。选择 完成 以保存变量设置。
6. 选择“确定”保存配置模板。
7. 新的配置模板将显示在 配置模板下。

创建配 置作业

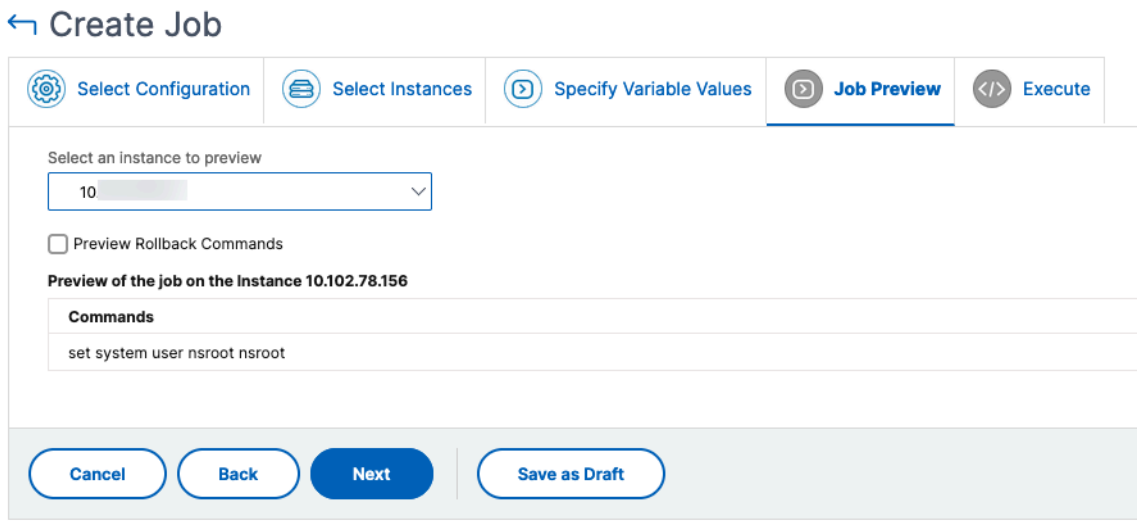
1. 在 NetScaler 控制台 GUI 中，导航到基础架构 **>** 配置作业。
2. 选择“创建作业”，然后单击新配置模板的“+”图标。选择下一步。



3. 选择必须修改密码的一个或多个 NetScaler 实例。



4. 在 选择实例 窗格中，选择实例，然后单击 下一步。
5. 在“指定变量值”窗格中，提供用户名和密码的值，然后单击“下一步”。
6. 在“作业预览”下，查看 NetScaler 控制台将在 NetScaler 实例上运行的实际 CLI 命令。如果预览看起来很好，请单击 下一步”。



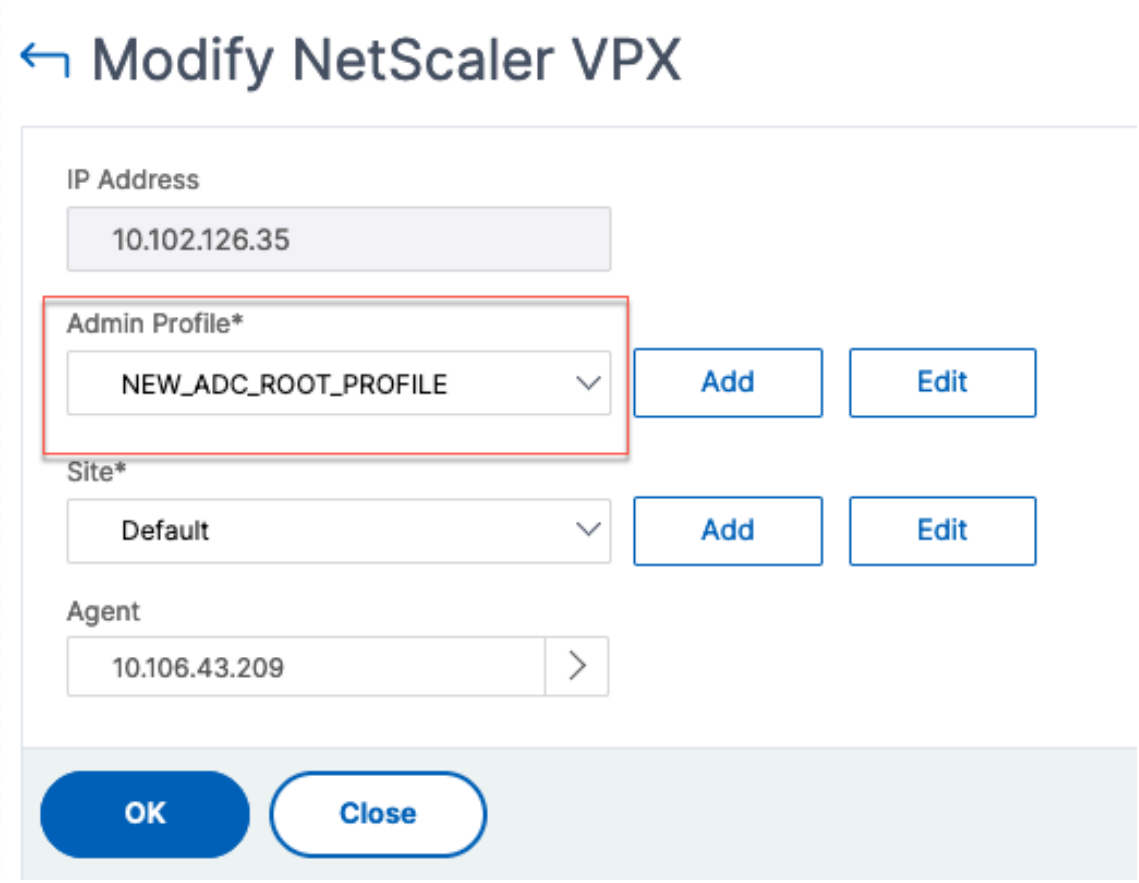
7. 在 执 行”窗格中，您可以选择立即运行作业或将其安排在以后。您也可以选择在所有选定实例上并行运行作业，也可以按顺序运行。提供执行详细信息后，选择“完成”。
8. 配置作业显示执行成功还是失败。
9. 选择作 业 并单击 详细信息。执行详细信息显示单个实例级别的状态。

修改管理员配置文件

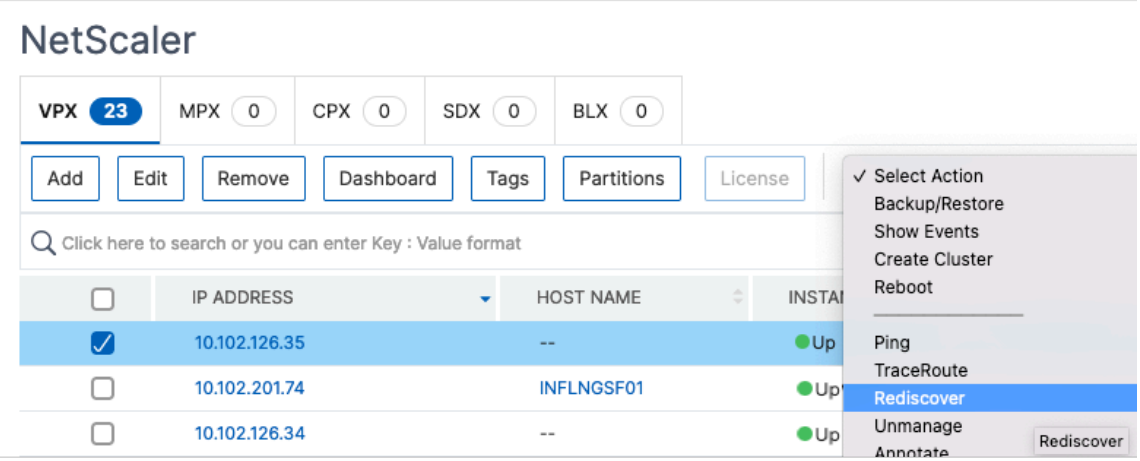
修改 NetScaler 密码后，必须添加和修改实例的管理配置文件。请按照以下步骤进行操作：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 单击“配置文件”可查看所有管理员配置文件。
3. 选择 添加 以创建管理员配置文件并提供新的 NetScaler 凭据。

4. 新创建的配置文件将显示在 管理员配置文件下。
5. 转到 网络 **>** 实例 **> NetScaler**。选择已修改密码的 NetScaler 实例，然后选择 编辑。
6. 选择新创建的配置文件名称，然后单击确定。



7. 再次选择实例，右键单击，然后选择 重新发现”。



您已成功更改密码。

有关更改 SDX 设备密码的信息，请参阅 如何更改 NetScaler SDX 根密码。

如何更改 **NetScaler SDX nsroot** 密码

January 29, 2024

有时，出于安全原因或密码轮换策略的合规性，您必须更改 NetScaler 设备的 nsroot 密码。

本文档描述了更改通过 NetScaler 控制台云管理的 NetScaler SDX 设备的 nsroot 密码所需的步骤。

如果您更改 NetScaler 密码，则必须修改与 NetScaler 关联的 NetScaler 控制台管理配置文件。NetScaler 控制台管理配置文件维护 NetScaler 凭据，用于与 NetScaler 设备进行基于 REST API、SSH、SCP 或 SNMP 的通信。通过管理配置文件，NetScaler 控制台管理 NetScaler SDX 设备。

更改密码

请按照以下步骤更改密码：

- 步骤 1. 从 SDX 管理服务 GUI 中更改 SDX 密码。
- 步骤 2. 修改与 SDX 关联的 NetScaler 控制台管理配置文件。

> 注意：
>
> 如果 SDX 设备也由其他工具管理，则还必须更改这些工具的证书。

从 **SDX** 管理服务 **GUI** 中更改 **SDX** 密码

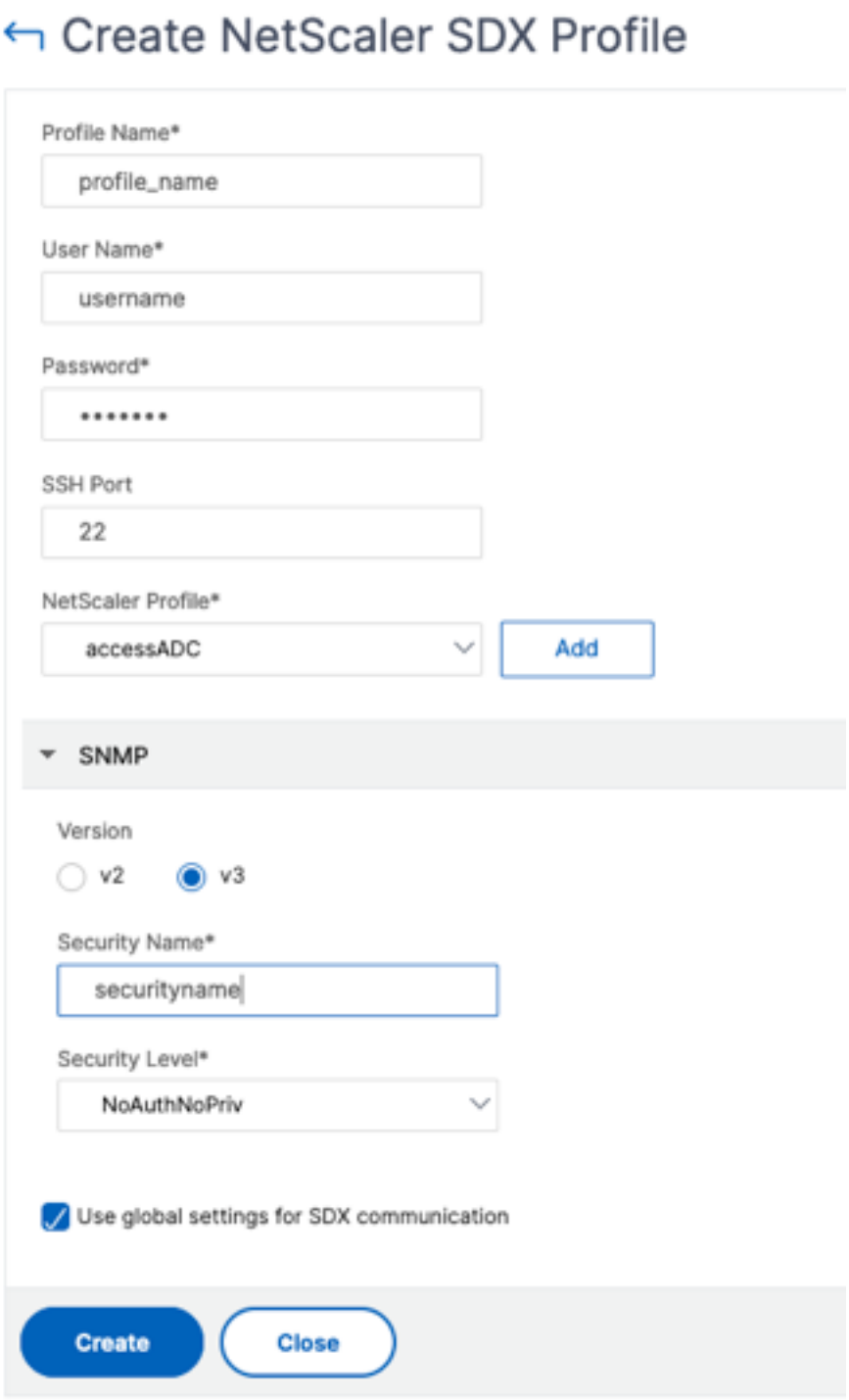
1. 在 SDX 管理服务中，导航到“系统”**>**“用户管理”**>**“用户”。
2. 选择要更改密码的用户名，然后单击“编辑”。
3. 选择“更改密码”。
4. 输入新密码并单击“确定”。
5. SDX 密码已更改

修改 **NetScaler** 控制台管理配置文件

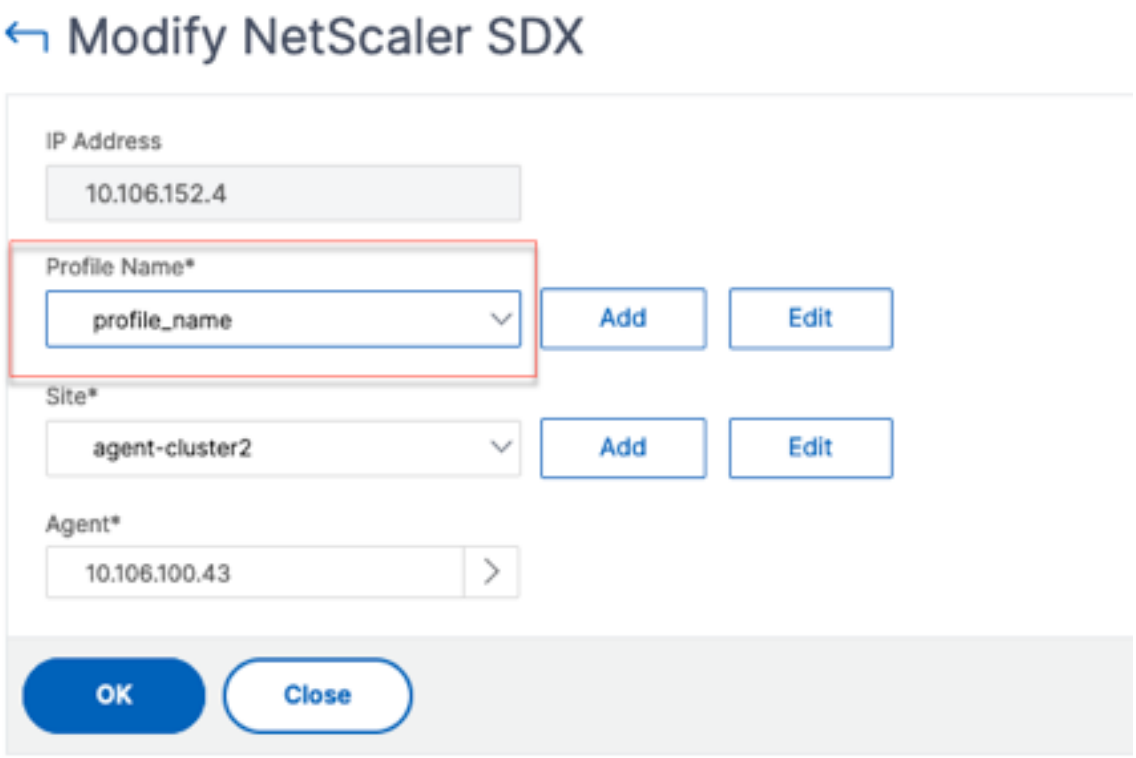
修改 SDX 密码后，必须修改实例的管理员配置文件。请按照以下步骤进行操作：

1. 导航到 基础结构 **>** 实例控制面板 **> NetScaler > SDX**。
2. 选择 配置文件 以查看所有管理员配置文件。
3. 选择“添加”以创建管理员配置文件。

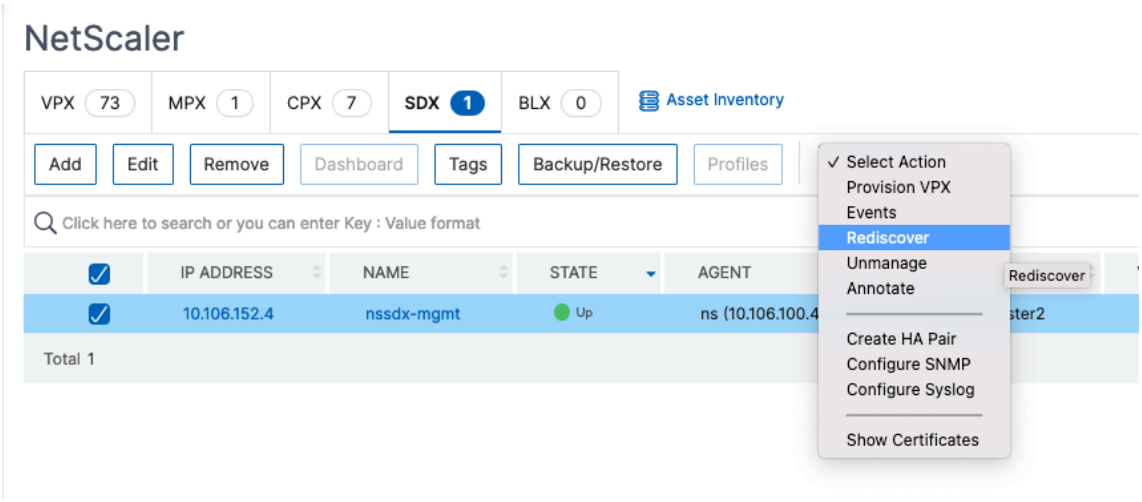
4. 提供新的 NetScaler 凭据，然后单击“创建”。



5. 新创建的配置文件将显示在 管理员配置文件下。
6. 转到 网络 **>** 实例 **> NetScaler > SDX**。选择密码已修改的实例，然后选择 编辑。
7. 选择新创建的配置文件名称，然后单击“确定”。



8. 再次选择实例，右键单击，单击“重新发现”。



您已成功更改密码。

有关更改 SDX 设备密码的信息，请参阅 如何更改 NetScaler MPX 或 VPX 根密码。

如何为 **NetScaler** 实例生成技术支持包

January 29, 2024

为了帮助分析和解决 NetScaler 实例的任何问题，可以在该实例上生成一个技术支持包并将该包发送给 Citrix 技术支持。技术支持包是系统配置数据和统计数据的 zip tar 存档。技术支持包从您生成捆绑包的 NetScaler 实例中收集以下数据：

- 配置文件。/flash/nsconfig 目录中的所有文件。
- `newnslog` 文件。当前正在运行 `newnslog` 的文件和一些以前的文件。为了最大限度地减少存档文件的大小，`newnslog` 集合限制为 500 MB、6 个文件或 7 天，以先发生者为准。如果需要较旧的数据，则可能需要手动收集。
- 日志文件。/var/log/messages 中的文件、/var/log/ns.log 以及 /var/log 和 /var/nslog 下的其他文件。
- 应用程序核心文件。上周在 /var/core 目录中创建的文件（如果有）。
- 某些 CLI 的输出显示命令。
- 一些 CLI stat 命令的输出。
- BSD shell 命令的输出。

您还可以将技术支持包安全地上载到 Citrix 技术支持服务器。从 NetScaler 14.1 版本 8.x 版本开始，在上载技术支持包之前，您必须生成身份验证令牌。在之前的版本中，您可以使用 Citrix 用户名和密码上载技术支持包。

要生成身份验证令牌，请执行以下操作：

1. 启动浏览器并输入以下 URL- https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600。
2. 使用多因素身份验证登录。

   > 注意：
   >
   > 有关如何注册多因素身份验证的信息，请参阅 如何注册多因素身份验证 (MFA)。

3. 单击“复 制”复制屏幕上显示的身份验证令牌。该令牌的有效期为 3600 秒（1 小时）。令牌允许的最大长度为 1023 个字符。

复制身份验证令牌后，使用 GUI 上载文件。

要使用 GUI 上载技术支持包，请执行以下操作：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 选择一个 NetScaler 实例。
3. 从“选择 操作”中选择“生成技术支持文件”。
4. 单击“生成技术支持文件”。
5. 使用作用域选项来指定是要收集当前节点、所有群集节点上的数据，还是要收集指定分区的数据。
6. 选择“上载收集器档案”。
7. 在“**My Citrix** 帐户”部分，在 **Citrix** 身份验证令牌字段中输入身份验证令牌。
8. 单击“创建技术支持”。

事件

January 29, 2024

当将 Citrix Application Delivery Controller (NetScaler) 实例的 IP 地址添加到 NetScaler 控制台时，NetScaler 控制台会发送 NITRO 调用，并隐式地将自己添加为陷阱目标，供该实例接收陷阱或事件。

事件表示托管 NetScaler 实例上发生的事件或错误。例如，当系统出现故障或配置更改时，NetScaler 控制台服务器上会生成和记录一个事件。在 NetScaler 控制台中收到的事件显示在事件摘要页面（基础架构 事件）上，所有活动事件显示在 事 件消息页面（基础架构 **>** 事件 事件消息）中。

NetScaler 控制台还会检查实例上生成的事件，以形成不同严重级别的警报并将其显示为消息，其中一些可能需要立即关注。例如，系统故障可以归类为“严重”事件严重性，可以立即解决。

可以配置规则以监视特定事件。通过规则，可以更轻松地监视在 NetScaler 基础结构中生成的各种事件。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的筛选条件时，将运行与该规则关联的操作。您可以创建筛选器的条件包括：严重性、NetScaler 实例、类别、故障对象、配置命令和消息。

您还可以确保在特定的时间间隔内针对某个事件触发多个通知，直到事件被清除。作为额外措施，您可能希望使用特定主题行、用户消息自定义电子邮件并上载附件。

使用事件控制板

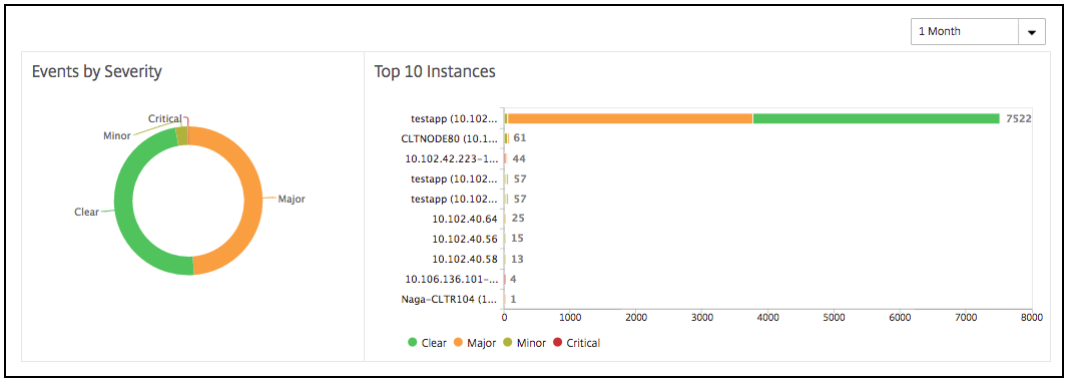
March 10, 2024

作为网络管理员，您可以查看 Citrix Application Delivery Controller (NetScaler) 实例上的配置更改、登录条件、硬件故障、阈值违规和实体状态更改等详细信息，以及特定实例上的事件及其严重性。您可以使用 NetScaler 控制台的事件控制面板查看为所有 NetScaler 实例的关键事件严重性详细信息而生成的报告。

要查看事件控制板上的详细信息：

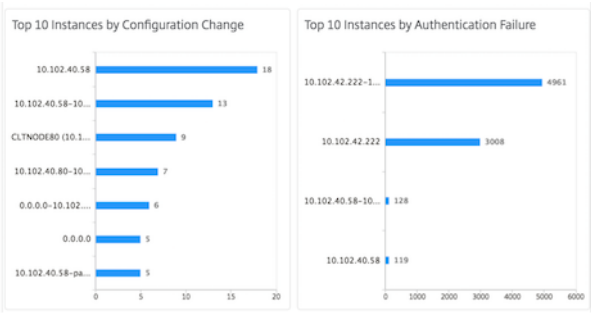
导航到 基础结构 **>** 事件 **>** 报告。

控制板上的“Top 10 Devices”（前 10 位的设备）图中显示按实例上生成的事件数排在前 10 位的实例的报告。您可以单击图表上的实例以查看事件严重性的更多详细信息。

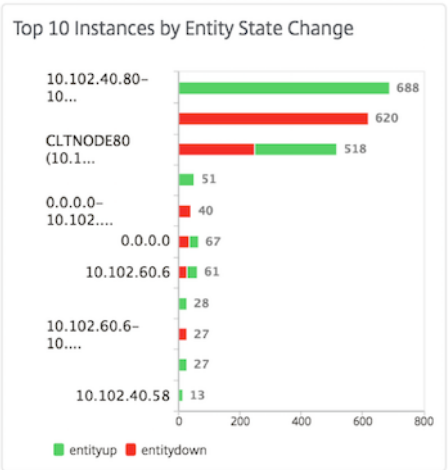


您可以导航到 NetScaler 实例类型（基础结构 **>** 事件 **>** 报告 NetScaler/C **itrix ADC SDX/NetScaler SDX/NetScaler**）查看以下内容，查看更多详细信息：

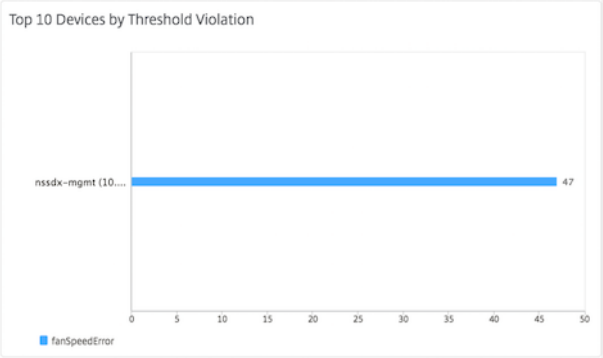
- Top 10 devices by hardware failure（按硬件故障排在前 10 位的设备）
- Top 10 devices by configuration change（按配置变更排在前 10 位的设备）
- Top 10 devices by authentication failure（按身份验证失败排在前 10 位的设备）



- Top 10 devices by entity state changes（按实体状态变化排在前 10 位的设备）



- Top 10 devices by threshold violation（按阈值违反排在前 10 位的设备）



要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

> 注意：
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

创建事件规则

May 9, 2024

可以配置规则以监视特定事件。规则可以更轻松地筛选基础结构中生成的事件。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的筛选条件时，将运行与该规则关联的操作。

您可以为以下条件创建过滤器：

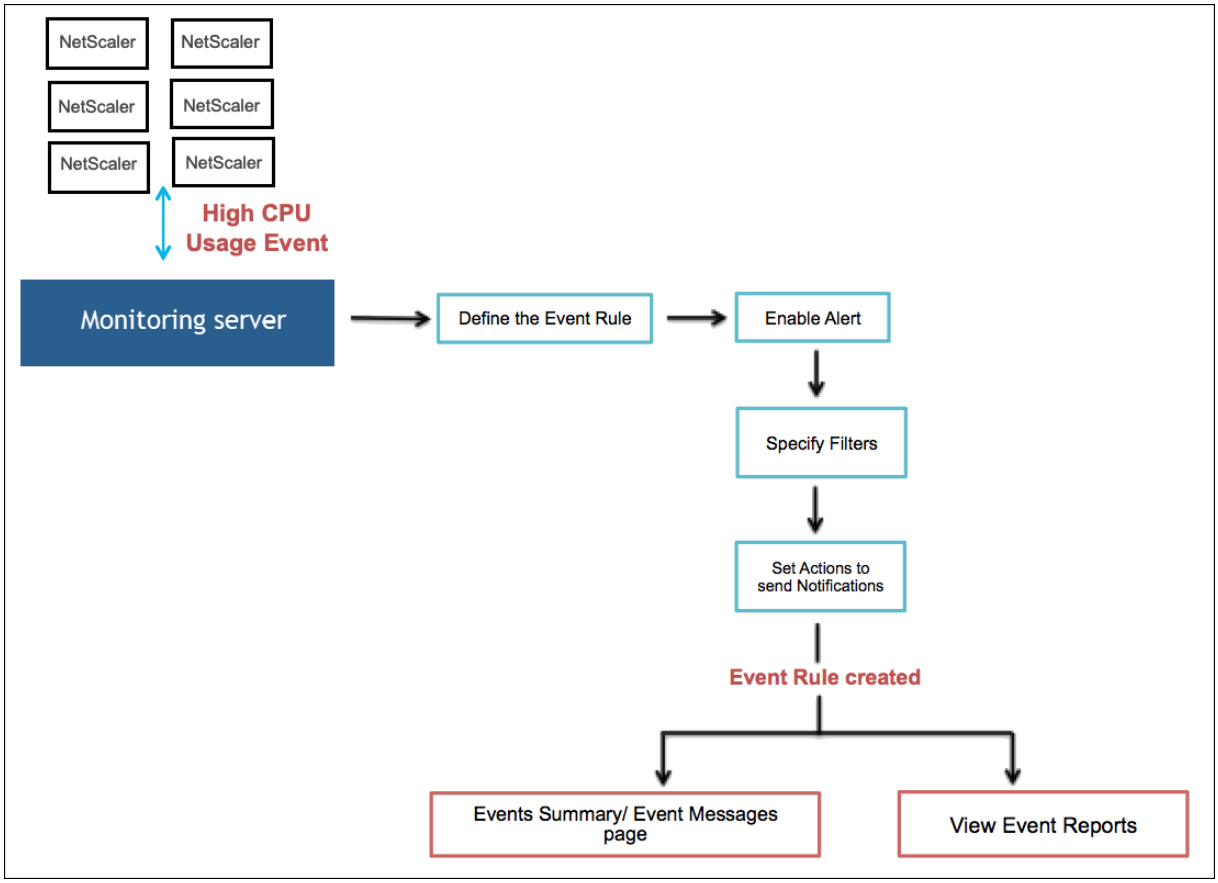
- 严重性
- Citrix Application Delivery Controller (NetScaler) 实例
- 类别
- 失败对象
- 配置命令
- 消息

创建事件后，您可以为事件分配操作。有关详细信息，请参阅 添加事件规则操作。

例如，作为管理员，您可能需要监视 NetScaler 实例上的“高 CPU 使用率”事件，这可能会导致中断。您可以执行以下任何操作来接收通知：

- 创建监视实例的规则，并在规则中添加操作以在发生此类事件时接收通知。
- 安排规则以按特定间隔监视实例。因此，当此类事件在该间隔内发生时，您会收到通知。

下图说明了事件规则的工作流程。



配置事件规则

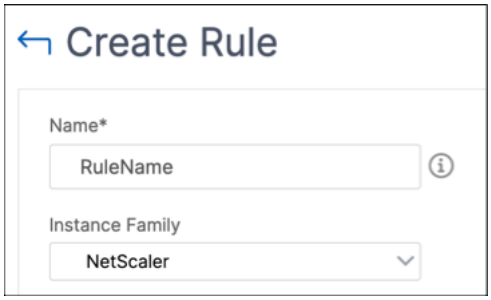
要配置事件规则，请导航到基础架构 **>** 事件 **>** 规则，然后单击添加。在“创建规则”页面中，执行以下任务：

1. 指定名称和实例系列
2. 配置事件年限
3. 选择规则检测到的事件的严重性
4. 指定事件的类别
5. 指定应用规则的 NetScaler 实例
6. 选择失败对象
7. 指定高级筛选器
8. 指定规则检测到事件时采取的操作

步骤 **1**-指定名称和实例系列

1. 名称。输入事件规则的名称。
2. 实例系列。从实例系列下拉列表中选择一个实例系列。

   您可以按 实例系列 筛选事件规则，以跟踪 NetScaler 控制台从中接收事件的 NetScaler 实例。



步骤 **2**-配置事件年限

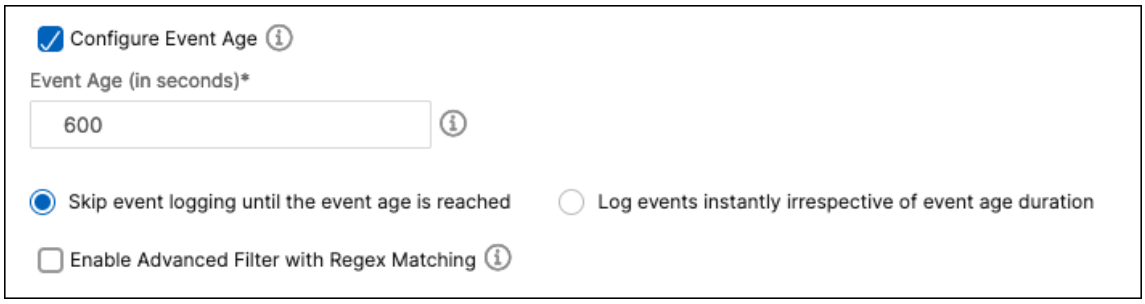
1. 事件期限。指定 NetScaler 控制台刷新事件规则的时间间隔（以秒为单位）。

   例如，您希望每当您的 NetScaler 实例出现 60 秒或更长时间的“高 CPU 使用率”事件时发送一封电子邮件。您可以将事件时长设置为 60 秒。现在，每当您的 NetScaler 实例出现 60 秒或更长时间的“高 CPU 使用率”事件时，您都会收到一封电子邮件通知。

   > 注意：
   >
   > 事件年限是必填字段。事件持续时间的最小值为 60 秒。如果将“事件时期”字段留空，则事件规则将在事件发生后立即应用。

2. 选择以下选项之一来追踪您的活动：

   - 在达到事件期限之前跳过事件记录。在指定事件期限之前发生的事件不会记录在 NetScaler 控制台服务器数据库中。当达到事件年龄时，事件将记录在数据库中，并触发配置的事件操作。
   - 无论事件持续时间长短，都可立即记录事件。无论指定的事件时长如何，所有事件都记录在 NetScaler 控制台服务器数据库中。达到事件年限后，将触发已配置的事件操作。



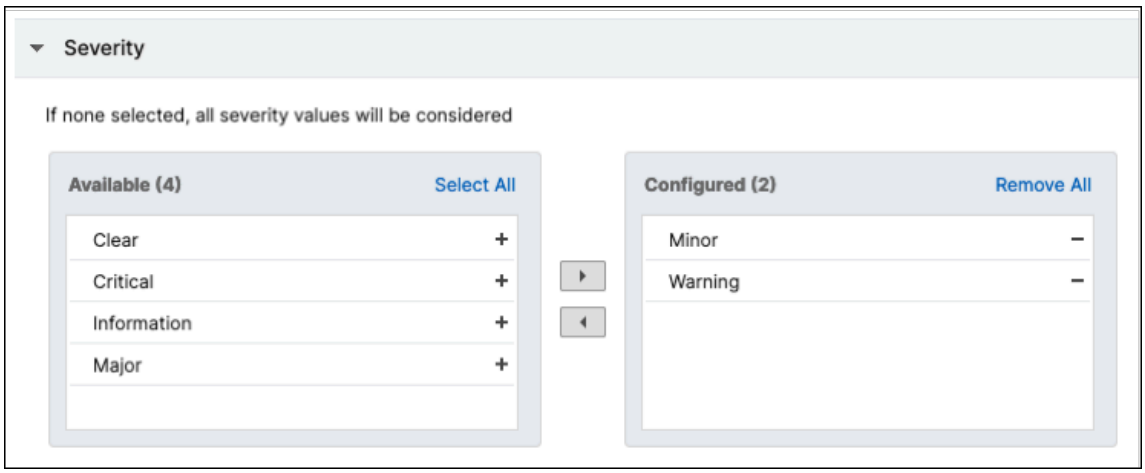
3. 启用带有正则表达式匹配的高级过滤器。选择此选项可包括除星号 (*) 模式匹配之外的正则表达式。此选项适用于故障对象、配置命令和消息。

第 **3** 步-选择事件的严重程度

- 在“严重性”部分中，为您的事件规则选择严重性。

  可以定义以下级别的严重性：Critical（严重）、Major（重大）、Minor（较小）、Warning（警告）、Clear（清除）及 Information（信息）。

  > 注意：
  >
  > 您可以为通用事件和高级特定事件配置严重性。要修改在 NetScaler 控制台上管理的 NetScaler 实例的事件严重性，请导航到基础架构 > 事件 > 事件设置。选择要为其配置事件严重性的 类别，然后单击 配置严重性。分配新的严重性级别，然后单击确定。

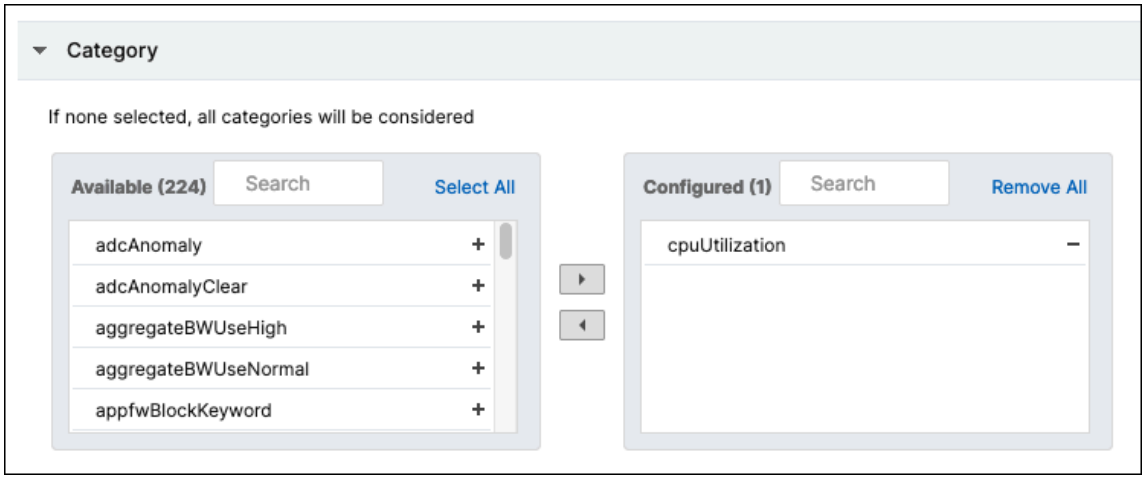


步骤 **4**-指定事件类别

您可以指定 NetScaler 实例生成的事件的类别或类别。所有类别都在 NetScaler 实例上创建。然后，这些类别将映射到可用于定义事件规则的 NetScaler 控制台。

- 选择要考虑的类别并将其从“可用”表移至“已配置”表。

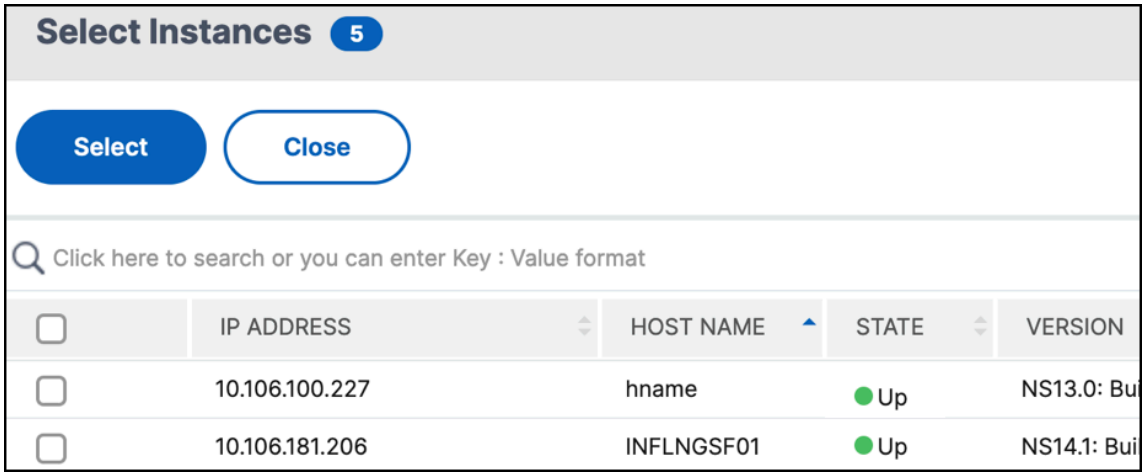
  在示例中，必须从显示的表格中选择“cpuUtilization”作为事件类别。



步骤 **5-**指定 **NetScaler** 实例

在“实例”部分中，执行以下操作：

1. 单击 选择实例。在“选择实例”页面中，选择要为其定义事件规则的 NetScaler 实例的 IP 地址。
2. 单击 **Select**（选择）。



步骤 **6-**选择失败对象

失败对象是已为其生成事件的实体实例或计数器。

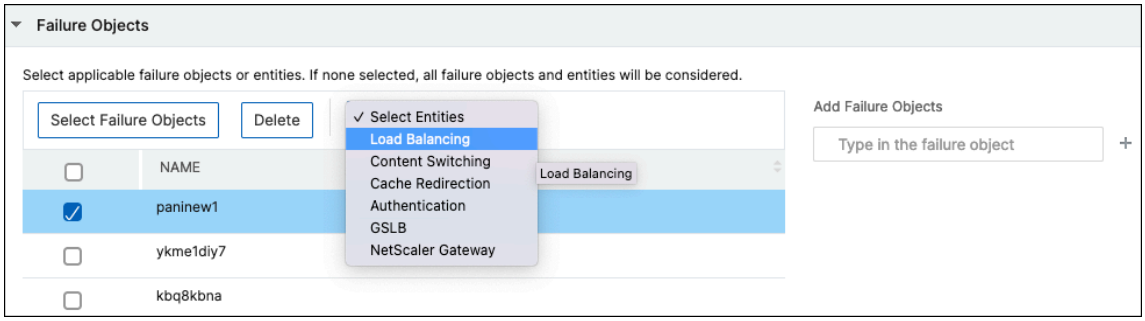
1. 单击“选择失败对象”。
2. 在“失效对象”页面中，从列表中选择一个失效对象。单击 **Select**（选择）。
3. 要添加失败对象，请在添加失败对象中输入正则表达式。根据指定的正则表达式，失败对象会自动添加到列表中。

> 重要：
>
> 要使用正则表达式列出失败对象，请在步骤 1 中选择启用带有正则表达式匹配的高级筛选器。

高级筛选器允许您快速跟踪故障对象上的问题并确定问题的原因。例如，如果用户遇到登录问题，则失败对象是用户名或密码，例如 `nsroot`。

4. 要添加实体，请从“选择实体”中选择一个实体。

   该列表可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、证书相关事件的证书名称等。

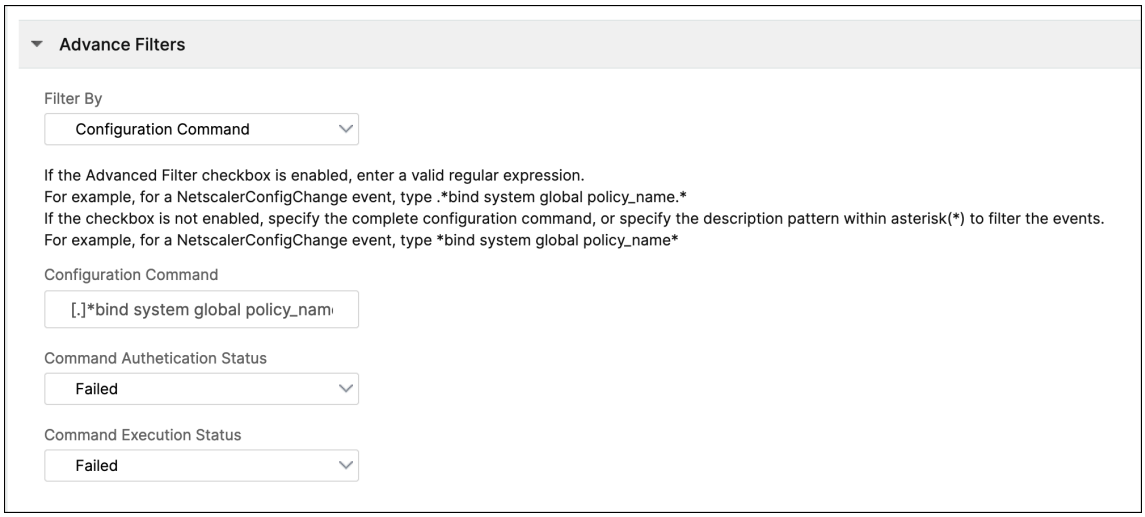


步骤 7-指定高级筛选器

您可以使用高级过滤器进一步筛选事件规则。选择以下过滤器之一：

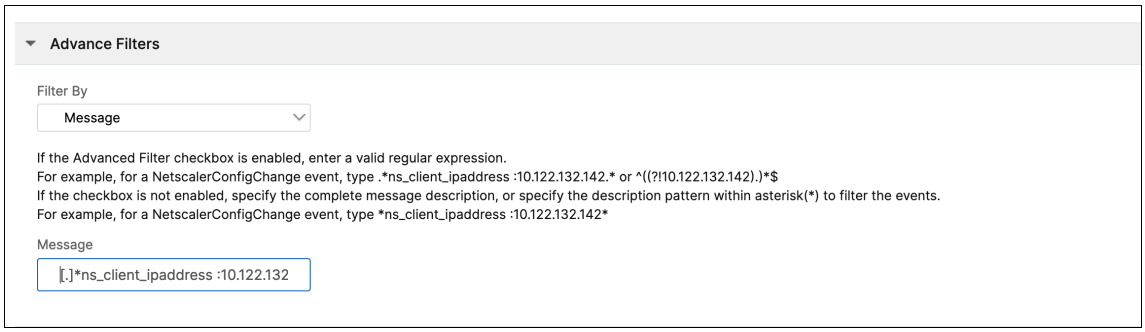
- 配置命令 - 指定完整的配置命令，或指定用于筛选事件的正则表达式。

  您还可以按命令的身份验证状态及其执行状态筛选事件规则。例如，对于 `NetscalerConfigChange event`，请键入 `[.]*bind system global policy_name[.]*`。



- 消息 - 指定完整的消息描述，或指定正则表达式来筛选事件。

例如，对于 NetscalerConfigChange 事件，请键入 [.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)。



> 重要：
>
> 要使用除星号 (*) 模式匹配之外的正则表达式筛选配置命令和消息，请在步骤 1 中选择使用正则表达式匹配启用高级筛选器。

步骤 8-添加事件规则操作

您可以添加事件规则操作来为事件分配通知操作。当事件满足您在步骤 7 中设置的已定义筛选条件时，就会发送或完成这些通知。

1. 单击“添加操作”。
2. 在“添加事件操作”页面中，您可以添加以下事件操作：

- 发送电子邮件操作
- Send Trap Action（发送陷阱操作）
- Run Command Action（运行命令操作）
- Execute Job Action（执行作业操作）
- Suppress Action（阻止操作）
- 发送 Slack 通知
- 发送 PagerDuty 通知
- 发送 ServiceNow 通知

发送电子邮件操作

选择“发 送电子邮件操作”时，当事件满足定义的筛选条件时，将触发电子邮件。

1. 电子邮件分发列表。选择电子邮件分发列表。要添加分发列表，请单击“添加”。

a) 在“创建电子邮件通讯组列表”页面中，执行以下操作：

i. 名称。为分发列表添加一个名称。

ii. 电子邮件服务器。选择电子邮件服务器。您也可以添加服务器或编辑现有服务器。

iii. 发件人。添加发件人的电子邮件地址。

iv. 收件人。添加收件人的电子邮件地址。您还可以指定要包含在“抄送”和“密件抄送”列表中的电子邮件地址。

v. 单击创建。

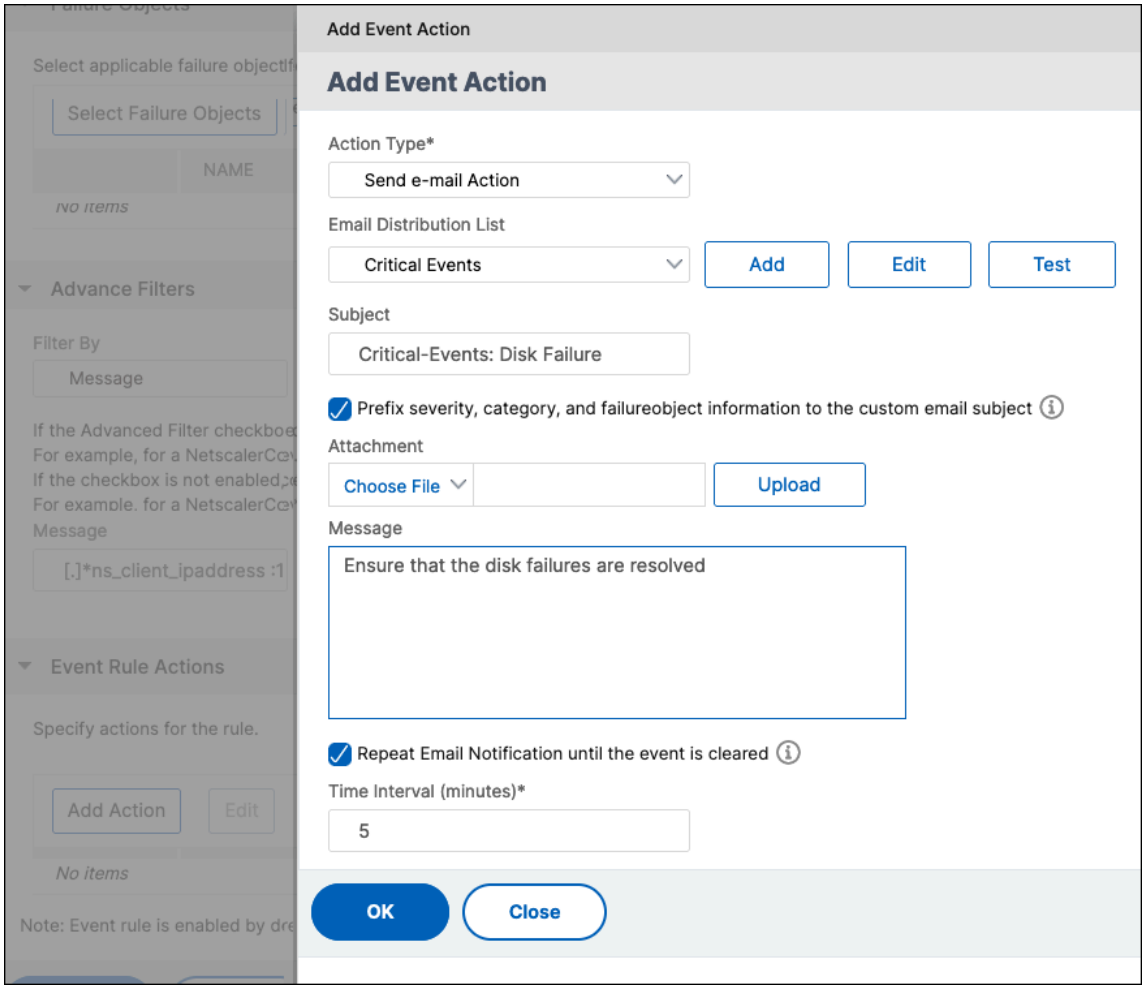
2. 主题。为您的电子邮件添加主题行，例如受影响实体的名称，即失败对象的名称。此主题行提供有关发生这些事件的虚拟服务器的信息。

> 注意：
>
> 如果您不添加主题行，则会显示默认主题行。默认主题行仅提供有关事件严重性、事件类别和失败对象的信息。发生事件的虚拟服务器的名称不可用。

3. 附件。将附件上载到您的电子邮件中。当传入事件与配置的规则匹配时，将发送此附件。

4. 测试。配置电子邮件服务器、关联的分布式列表和其他设置后，单击此按钮发送测试电子邮件。此选项允许您测试已配置的设置

5. 重复电子邮件通知，直到事件被清除。选择此选项可确保不会错过关键事件的电子邮件通知。此选项会重复发送符合您所选条件的事件规则的电子邮件。例如，您为涉及磁盘故障的实例创建了事件规则。如果您想在问题解决之前收到通知，请选择重复接收有关这些事件的电子邮件通知。



6. 单击确定。

> 注意：
>
> 您还可以通过导航到“设置”>“通知”>“电子邮件”来添加电子邮件通讯组列表。单击“添加”并创建列表。

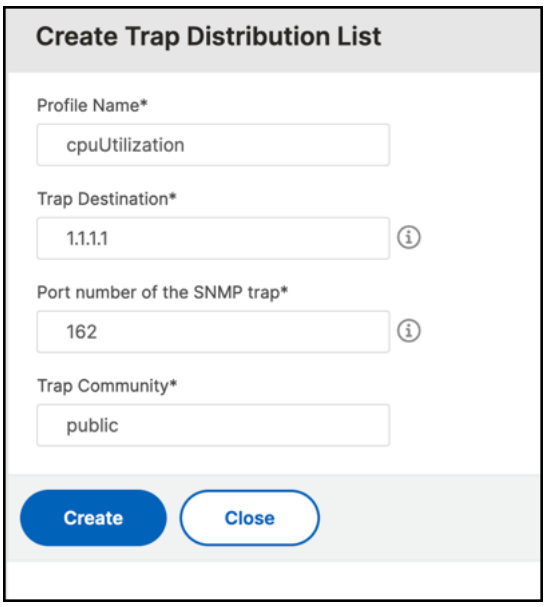
Send Trap Action（发送陷阱操作）

选择发送陷阱操作事件操作类型时，SNMP 陷阱将被发送或转发到外部陷阱目标。当事件满足定义的过滤条件时，陷阱消息将发送到特定的陷阱侦听器。

1. 陷阱分发列表。选择陷阱分发列表（或陷阱目的地和陷阱配置文件详细信息）。要创建陷阱分发列表，请单击“添加”。
2. 在“创建陷阱分发列表”页面中，执行以下操作：
   a) 配置文件名称。输入配置文件名称。
   b) 陷阱目的地。输入应接收陷阱消息的实例的名称或 IP 地址。

c) **SNMP** 陷阱的端口号。输入端口号。

d) 陷阱社区。输入实例所属的组。



e) 单击创建。

3. 单击确定。

Run Command Action（运行命令操作）

选择“运行命令操作”事件操作 时，您可以为符合特定筛选条件的事件创建命令或脚本，该命令或脚本可在 NetScaler 控制台上运行。

您还可以为运行命令操作脚本设置以下参数：

参数	说明
$source	此参数对应于接收的事件的源 IP 地址。
$category	此参数对应于过滤器类别下定义的陷阱类型
$entity	此参数对应于已为其生成事件的实体实例或计数器。它可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、所有证书相关事件的证书名称。
$severity	此参数对应于事件的严重性。
$failureobj	失败对象会影响事件的处理方式，并确保故障对象按通知显示确切的问题。这可以用于快速追查问题以及确定失败的原因，而不是仅仅报告原始事件。

> 注意：
>
> 在命令执行过程中，这些参数将替换为实际值。

例如，假设您要在负载平衡虚拟服务器状态为“关闭”时设置运行命令操作。作为管理员，您可能需要通过添加另一台虚拟服务器来提供一种快速的解决方法。在 NetScaler 控制台中，您可以：

- 编写脚本 (.sh) 文件。

  以下是一个示例脚本 (.sh) 文件：

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
   application/json" -X POST -d $payload $url
```

- 将.sh 文件保存在代理上的任何永久位置。例如，/var。
- 在 NetScaler 控制台中提供.sh 文件位置，以便在满足规则条件时运行。

1. 在“命令执行列表”中，单击“添加”。

   屏幕上将显示“创建命令分发列表”页面。

   a) 配置文件名称。指定您选择的名称

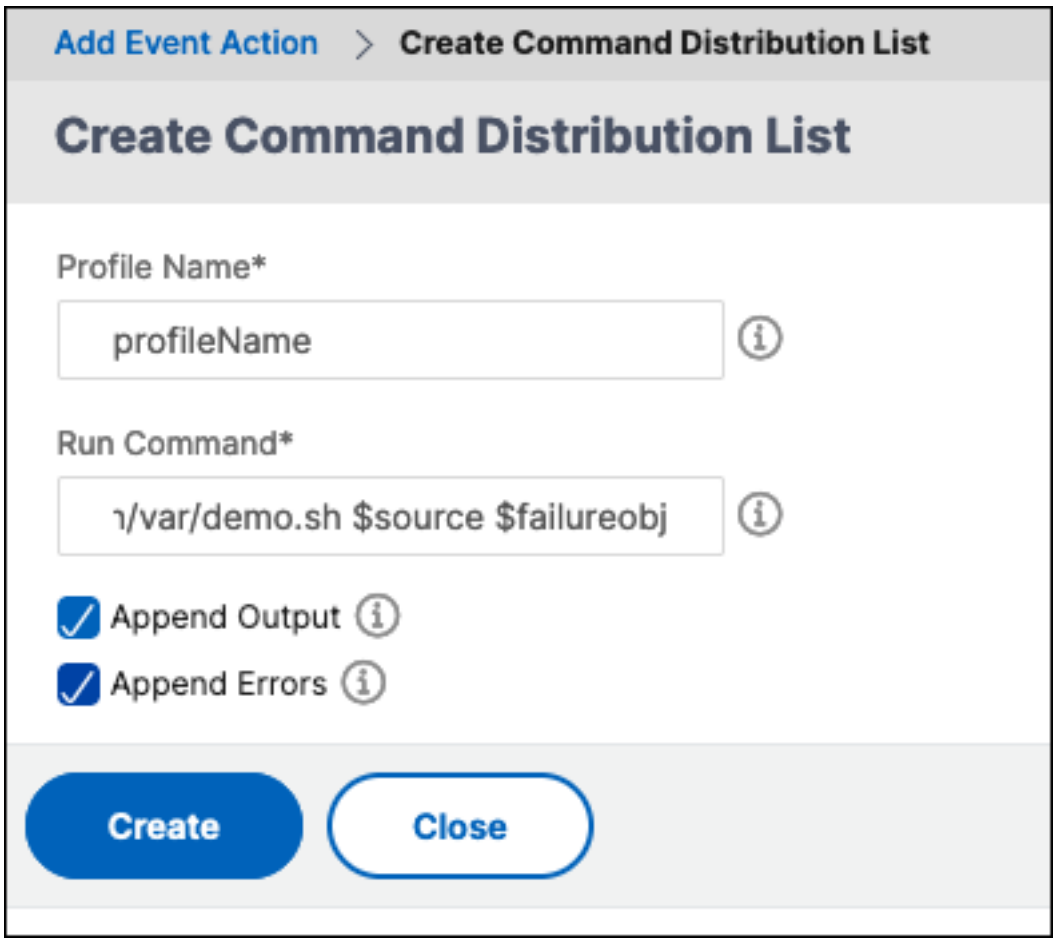
   b) 运行命令。指定必须运行脚本的代理位置。例如：sh/var/demo.sh $source $failureobj。

   c) 选择“追加输出”和“追加错误”

   > 注意：
   >
   > 如果要在 NetScaler 控制台服务器日志文件中存储运行命令脚本时产生的输出和错误（如果有），可以启用“追加输出”和“追加错误”选项。如果您未启用这些选项，NetScaler 控制台将丢弃运行命令脚本时生成的所有输出和错误。

   d) 单击创建。

2. 在添加事件操作页面中，单击确定。

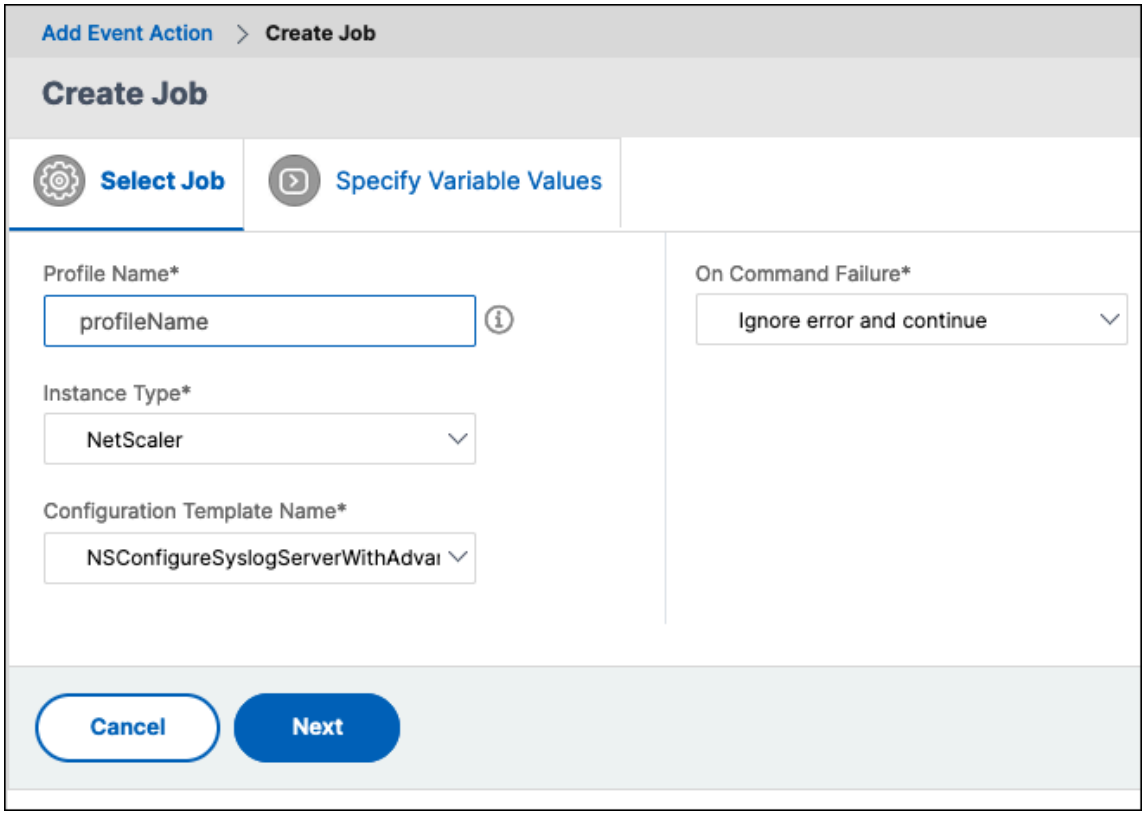


> 注意：
>
> 如果要在 NetScaler 控制台服务器日志文件中存储运行命令脚本时产生的输出和错误（如果有），可以启用“追加输出”和“追加错误”选项。如果您未启用这些选项，NetScaler 控制台将丢弃运行命令脚本时生成的所有输出和错误。

Execute Job Action（执行作业操作）

当您使用配置作业创建配置文件时，作业将作为内置作业运行，或者针对符合您指定的筛选条件的事件和警报，NetScaler 和 NetScaler SDX 实例将作为定制作业运行。

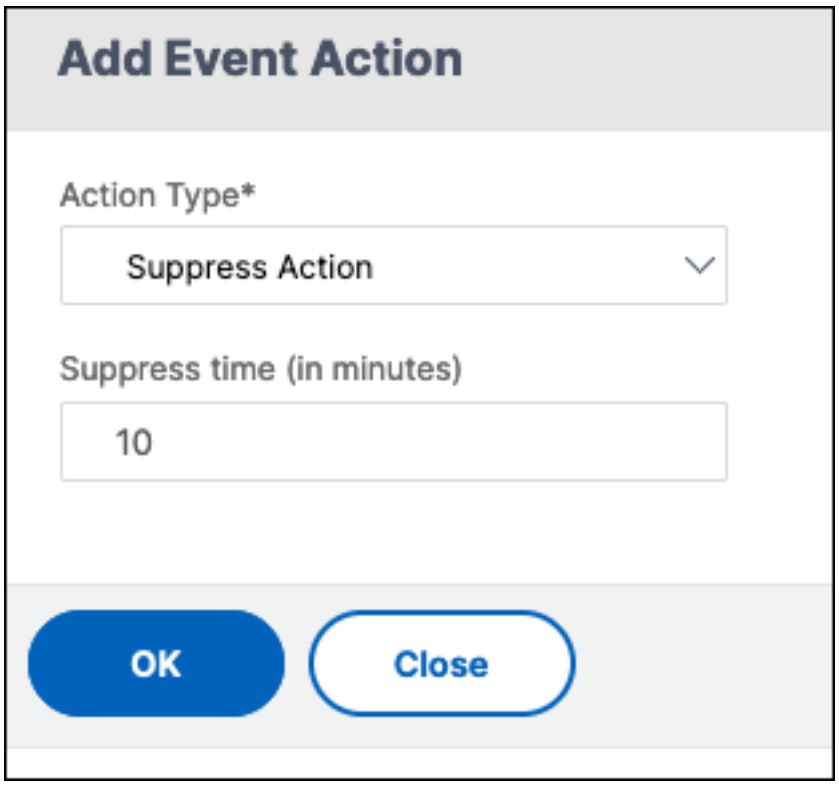
1. 在“工作配置文件列表”中，选择工作配置文件。要添加列表，请单击“添加”。
2. 在“创建作业”页面中，执行以下操作：
    a) 选择“作业”。创建配置文件，其中包含要在事件满足定义的筛选条件时运行的作业。指定配置文件名称、实例类型、配置模板以及任务命令失败时要执行的操作。
    b) 指定变量值。根据所选的实例类型和选择的配置模板，指定您的变量值。
    c) 单击“完成”创建作业。



3. 单击确定。

Suppress Action（阻止操作）

- 在抑制时间中，输入抑制或删除事件的时间段（以分钟为单位）。可以最短阻止事件 1 分钟。



> 注意：
>
> 您还可以将禁止时间配置为 0 分钟，这意味着无限时间。如果您未指定任何时长，则 NetScaler 控制台会将抑制时间视为零且永不过期。

发送 **Slack** 通知

配置 Slack 频道时，事件通知会发送到该频道。您可以配置许多 Slack 频道来接收这些通知

1. 在 **Slack** 配置文件列表中，选择一个 Slack 配置文件。要添加 Slack 配置文件，请单击“添加”。
2. 在 创建 **Slack** 配置文件页面中，执行以下操作：
   a) 配置文件名称。键入要在 NetScaler 控制台上配置的配置文件列表的名称
   b) 频道名称。键入要向其发送事件通知的 Slack 频道的名称。
   c) **Webhook URL**。键入您输入的频道的 Webhook URL。传入的 Webhook 是将来自外部来源的消息发布到 Slack 的简单方法。URL 在内部链接到频道名称。所有事件通知都将发送到该 URL，然后发布到所选的 Slack 频道。webhook 的一个例子如下：https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
   d) 单击创建。
3. 单击确定。

> 注意：
>
> 您也可以通过导航到“设置”>“通知”>“**Slack** 配置文件”来添加 Slack 配置文件。单击“添加”并创建配置文件。

发送 **PagerDuty** 通知

您可以在 NetScaler 控制台中将 PagerDuty 配置文件作为选项添加，以根据您的 PagerDuty 配置监视事件通知。使用 PagerDuty，您可以通过电子邮件、短信、推送通知和电话在注册号码上配置通知。

1. 在 **PagerDuty** 配置文件列表中，选择 PagerDuty 配置文件。要添加配置文件，请单击“添加”。
2. 在“创建 **PagerDuty** 配置文件”页面中：
    a) 配置文件名称。输入您选择的配置文件名称。
    b) 集成密钥。输入 集成密钥。
        您可以从您的 PagerDuty 门户获取集成密钥。
    c) 单击创建。

在 NetScaler 控制台中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。有关更多信息，请参阅 PagerDuty 文档。

可以选择您的 PagerDuty 配置文件作为获取以下功能通知的选项之一：

- 事件—为 NetScaler 实例生成的事件列表。
- 许可证—当前处于活动状态、即将到期等的许可证列表。
- **SSL** 证书—添加到 NetScaler 实例的 SSL 证书列表。

使用案例：

假设您想执行以下操作的场景：

- 向您的 PagerDuty 配置文件发送通知。
- 在 PagerDuty 中将电话配置为一个选项以接收通知。
- 获取有关 NetScaler 事件的电话提醒。

创建 PagerDuty 配置。配置完成后，每当为 NetScaler 实例生成新事件时，您都会接到一个电话。通过调用，您可以决定：

- 确认事件
- 将其标记为已解决
- 上报给其他团队成员

发送 **ServiceNow** 通知

通过在 NetScaler 控制台 GUI 上选择 ServiceNow 配置文件，您可以为 NetScaler 控制台事件自动生成 ServiceNow 事件。必须在 NetScaler 控制台中选择 **ServiceNow** 配置文件才能配置事件规则。

在配置事件规则以自动生成 ServiceNow 事件之前，请将 NetScaler 控制台与 ServiceNow 实例集成。有关详细信息，请参阅为 ServiceNow 配置 ITSM 适配器。

1. 在 **ServiceNow** 配置文件中，从列表中选择 **Citrix_Workspace_SN** 配置文件。
2. 单击确定。

安排事件过滤器

March 10, 2024

为规则创建过滤器后，如果您不希望 NetScaler 控制台在每次生成的事件满足筛选条件时都发送通知，则可以将过滤器安排为仅在特定的时间间隔（例如每天、每周或每月）触发。

例如，如果为实例上的不同应用程序计划了在不同时间进行系统维持活动，实例可能会生成多个警报。

如果您为这些警报配置了过滤器并为这些过滤器启用了邮件通知，则当 NetScaler 控制台收到这些陷阱时，服务器会发送许多邮件通知。如果希望服务器仅在特定的时间段发送这些电子邮件通知，可以通过计划过滤器来实现。

要使用 **NetScaler** 控制台安排过滤器，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 事件 **>** 规则。
2. 选择要为其计划过滤器的规则，并单击 **View Schedule**（查看计划）。
3. 在 **Scheduled Rule**（计划的规则）页面上，单击 **Schedule**（计划）并指定以下参数：
   - 启用规则—选中此复选框可启用计划事件规则。
   - **Recurrence**（定期循环）- 计划规则的时间间隔。
   - 计划时间间隔（小时） -小时，计划规则的时间（使用 24 小时格式）。
4. 单击 **Schedule**（计划）。

修改报告的 **NetScaler** 实例上发生的事件的严重性

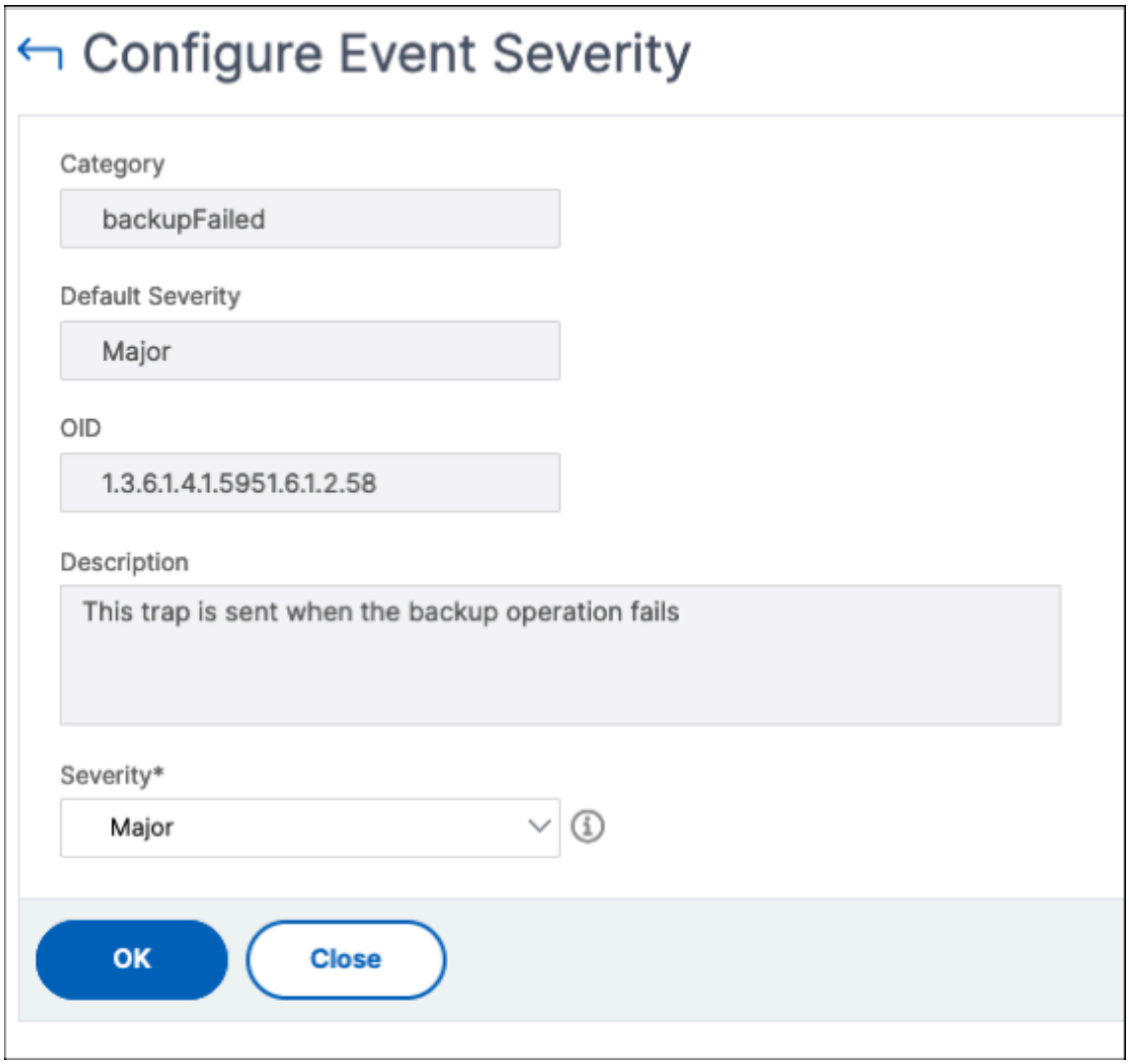
January 29, 2024

您可以管理在所有设备上生成的事件的报告，以便查看实例上特定事件的事件详细信息，并根据事件严重性查看报告。此外，您可以创建使用默认严重性设置的事件规则，也可以更改严重性设置。可以为一般事件和企业特定的事件配置严重性。

可以定义以下级别的严重性：Critical（严重）、Major（重大）、Minor（较小）、Warning（警告）及 Clear（清除）。

要修改事件严重性：

1. 导航到 基础结构 **>** 事件 **>** 事件设置。
2. 单击要修改的 NetScaler 实例类型的选项卡。然后，从列表中选择类别，然后单击 配置严重性。
3. 在 **Configure Event Severity**（配置事件严重性）中，从下拉列表中选择严重级别。
4. 单击确定。

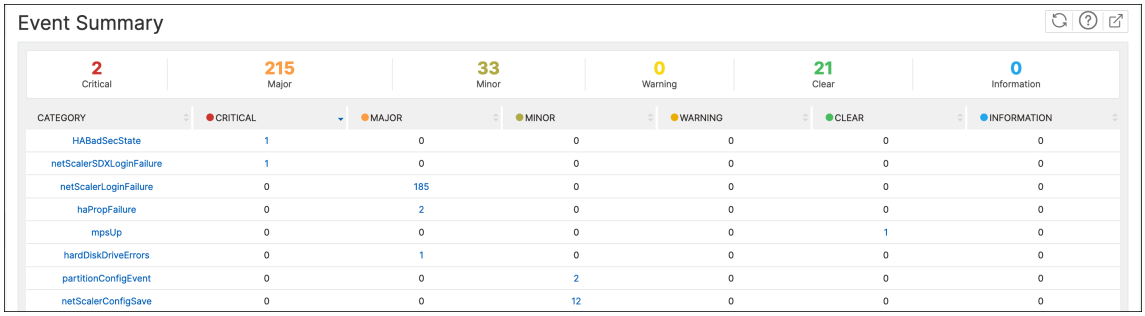


查看事件摘要

March 10, 2024

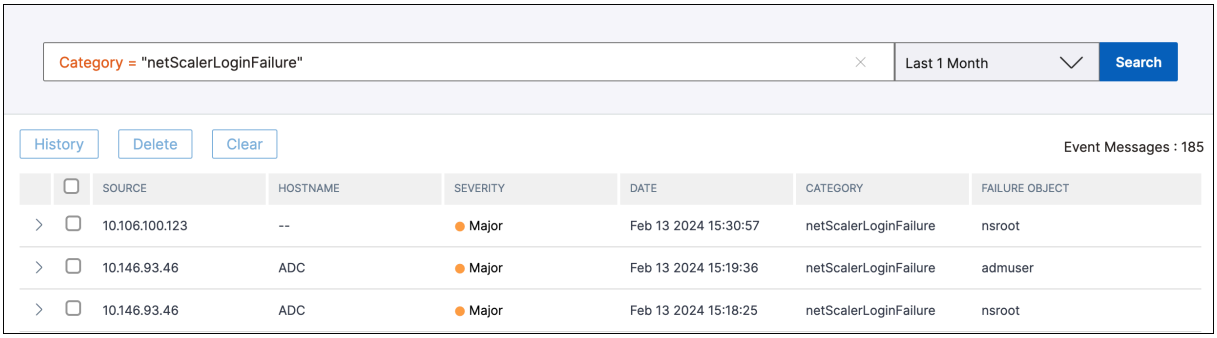
现在，您可以查看“事件摘要”页面，以监视在 NetScaler 控制台上收到的事件和陷阱。导航到 基础结构 > 事件。“Events Summary”（事件摘要）页面以表格形式显示以下信息：

- **NetScaler** 控制台收到的所有事件的摘要。这些事件按类别列出，不同的严重程度显示在不同的列中：严重、严重、次要、警告、清除和信息。例如，当 Citrix Application Delivery Controller (NetScaler) 实例出现故障并停止向 NetScaler 控制台发送信息时，就会发生严重事件。活动期间，系统会向管理员发送通知，说明实例关闭的原因、关闭的时间等。事件随后会记录在“事件摘要”页面上，您可以在该页面上查看摘要并访问事件的详细信息。



- 每个类别收到的陷阱数量。收到的陷阱数，按严重性分类。默认情况下，从 NetScaler 实例发送到 NetScaler 控制台的每个陷阱都有指定的严重性，但作为网络管理员，您可以在 NetScaler 控制台 GUI 中指定其严重性。

如果单击类别类型或陷阱，则会进入 事件 页面，在该页面上预先选择类别和严重性等筛选器。此页面显示有关事件的详细信息，例如 NetScaler 实例的 IP 地址和主机名、接收陷阱的日期、类别、故障对象、配置命令运行以及消息通知。



您可以配置 1 到 40 天之间的天数，以便在 NetScaler 控制台中查看该天数的事件。例如，如果您选择 30 天，NetScaler 控制台将显示 30 天的事件，30 天后，事件将被清除。要配置此事件设置，请导航到 设置 > 全局设置 > 数据保留策略。有关更多信息，请参阅 数据保留政策。

要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。

2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

> 注意：
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

显示事件严重性和 **SNMP** 陷阱详细信息

March 10, 2024

在 NetScaler 控制台中创建事件及其设置时，可以立即在“事件摘要”页面上查看该事件。同样，您可以在基础架构控制面板上详细查看和监视添加到 NetScaler 控制台服务器的所有 Citrix Application Delivery Controller（NetScaler）实例的运行状况、正常运行时间、模型和版本。

在基础结构控制板上，您现在可以屏蔽不相关的值，以便更轻松地查看和监视按严重性划分的事件、运行状况、正常运行时间、型号和 NetScaler 实例版本等信息。

例如，严重级别为“严 重”的事件可能很少发生。但是，如果您的网络上发生严重事件，您可能想要对事件的发生地点和时间进一步进行调查、故障排除和监视。如果您选择“Critical”（严重）以外的所有严重级别，则图形将仅显示发生的严重事件。此外，通过单击该图表，您将进入 基于严重性的事件 页面，在该页面中，您可以查看有关在您选择的持续时间内发生严重事件的所有详细信息：实例来源、日期、类别和在重要事件发生时发送的消息通知。

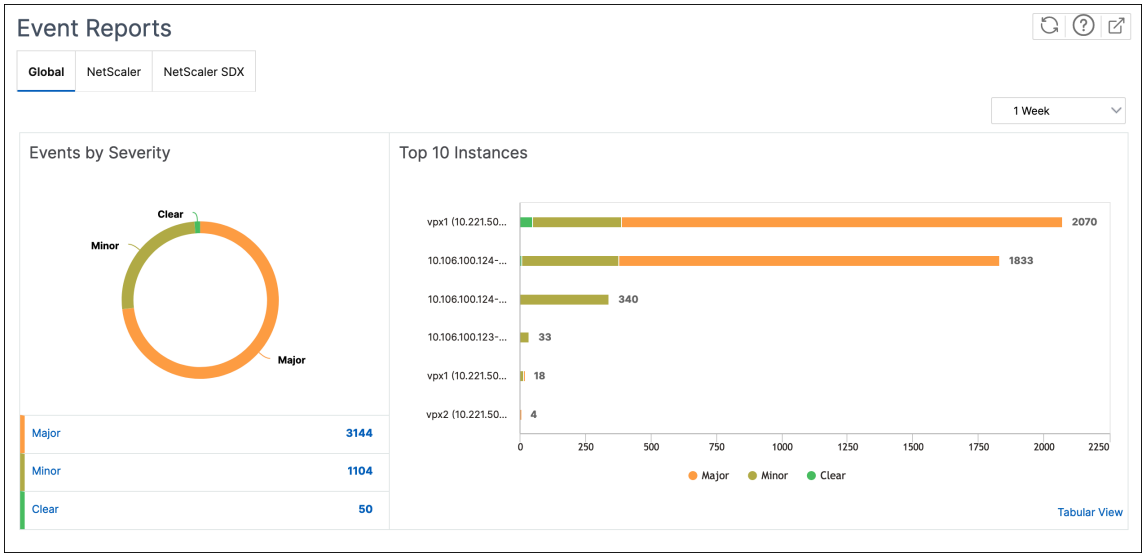
同样，您可以在控制板上查看 NetScaler VPX 实例的运行状况。您可以屏蔽实例已启动并运行的时间段，只显示实例停止工作的时间段。通过单击图表，您将进入该实例的页面，该页面已应用 了不服务 过滤器，并查看详细信息，例如主机名、每秒收到的 HTTP 请求数、CPU 使用率等。您还可以选择实例并查看实例控制面板了解更多详细信息。

要在 **NetScaler** 控制台中按严重性选择特定事件，请执行以下操作：

1. 使用您的管理员凭据登录 NetScaler 控制台。
2. 导航到 **Infrastructure**（基础结构）**> Instances**（实例）。

   或者，

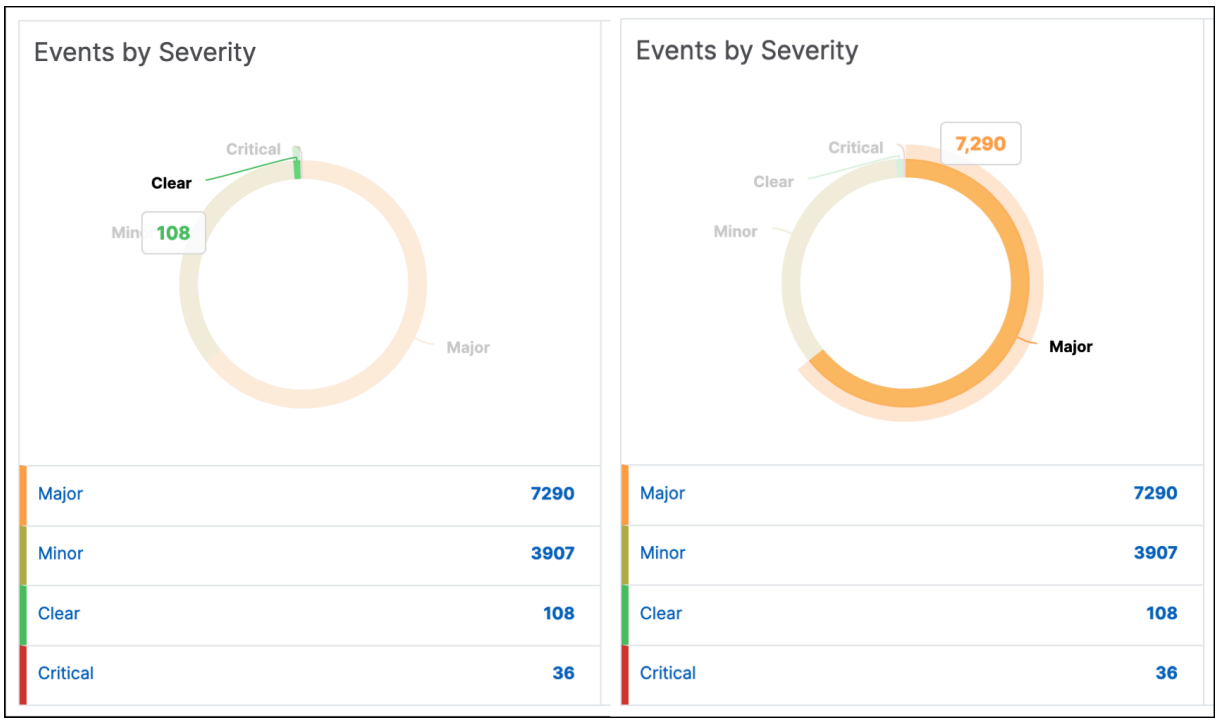
   导航到 基础结构 **>** 事件 **>** 报告。
3. 从页面右上角的下拉列表中，选择您要查看按严重性列出的事件的持续时间。



4. 按严重程度划分的事件圆环图按严重性显示了所有事件的可视化表示。不同类型的事件以不同的彩色部分表示，每个部分的长度对应于该严重性类型的事件总数。
5. 您可以单击圆环图表上的每个部分以显示相应的 基于严重性的事件 页面，该页面显示所选持续时间内所选严重性的以下详细信息：

    - 实例源
    - 事件日期
    - 由 NetScaler 实例生成的事件类别
    - 发送的消息通知

> 注意：
>
> 在甜甜圈图下方，您可以看到图表中显示的严重程度列表。默认情况下，圆环图显示所有严重性类型的所有事件，因此，列表中的所有严重性类型均突出显示。将鼠标悬停在严重性类型上，可以更轻松地查看和监视您选择的严重程度。

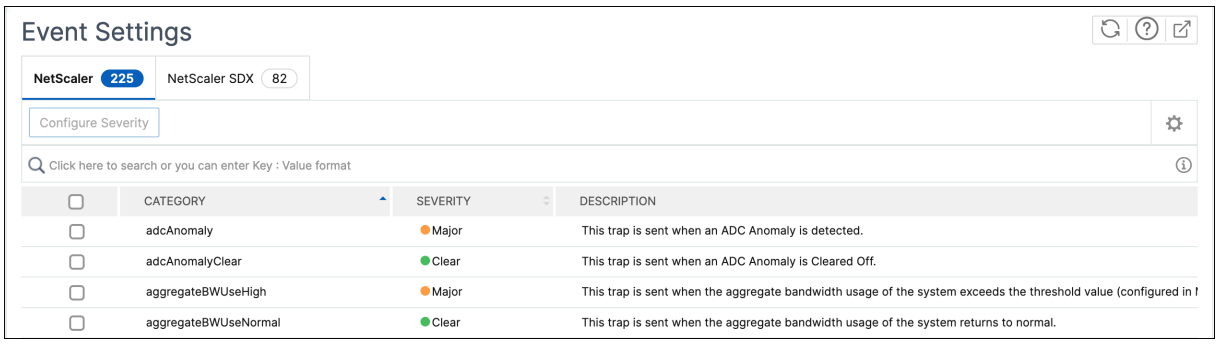


要在 **NetScaler** 控制台上查看 **NetScaler SNMP** 陷阱的详细信息，请执行以下操作：

现在，您可以在 NetScaler 控制台的“事件设置”页面上查看从其托管 NetScaler 实例接收到的每个 SNMP 陷阱的详细信息。导航到 基础结构 **>** 事件 **>** 事件设置。对于从您的实例接收的特定陷阱，您可以以表格形式查看以下详细信息：

- 类别 -指定事件所属实例的类别。
- 严重性 -事件的严重性由颜色及其严重性类型表示。
- 说明 -指定与事件关联的消息。

例如，陷阱类别为 **aggregateBWUseNormal** 的事件，该陷阱的描述显示为“当系统的总带宽使用量恢复正常”时，会发送此陷阱。



查看和导出系统日志消息

July 17, 2024

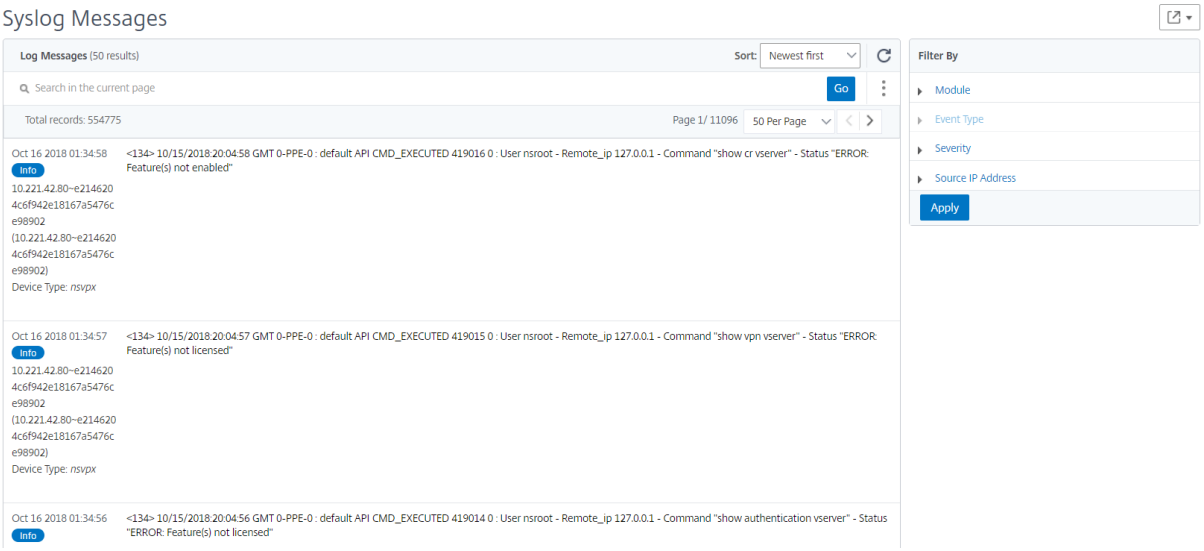
通过计划导出服务器上收到的所有系统日志消息，您无需登录 NetScaler 控制台即可查看系统日志消息。您可以以 PDF、CSV、PNG 和 JPEG 格式导出在 Citrix 应用程序 Delivery Controller (NetScaler) 实例上生成的系统日志消息。此外，您可以安排在不同的时间间隔将这些报告导出到指定的电子邮件地址。

查看系统日志消息

您可以查看在托管 NetScaler 实例上生成的所有 syslog 消息。要查看消息，必须将实例配置为将系统日志消息重定向到 NetScaler 控制台服务器。syslog 消息集中存储在数据库中，并可在 Syslog 查看器中用于审核目的。您可以合并这些日志记录信息，然后从收集的数据中派生报告以进行分析。

还可以配置 syslog 来记录不同类型的事件。

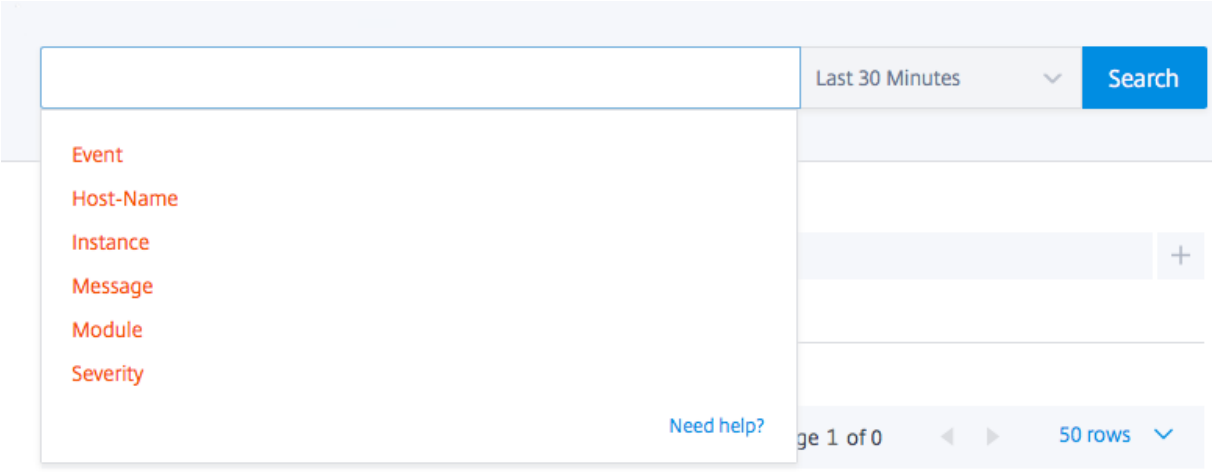
要查看 Syslog 查看器，请导航到 基础结构 **>** 事件 **> Syslog** 消息。选择适当的过滤器，查看系统日志消息。



搜索系统日志消息

您可以使用筛选器搜索 syslog 消息和审核日志消息，以缩小结果范围并实时准确找到您要查找的内容。

要在系统日志消息中搜索 NetScaler 控制台软件中存在的所有 NetScaler 实例，请从 NetScaler 控制台 GUI 中导航到基础架构 **>** 事件 **> syslog** 消息。新的过滤器类别包括实例、模块、事件、严重性和消息。



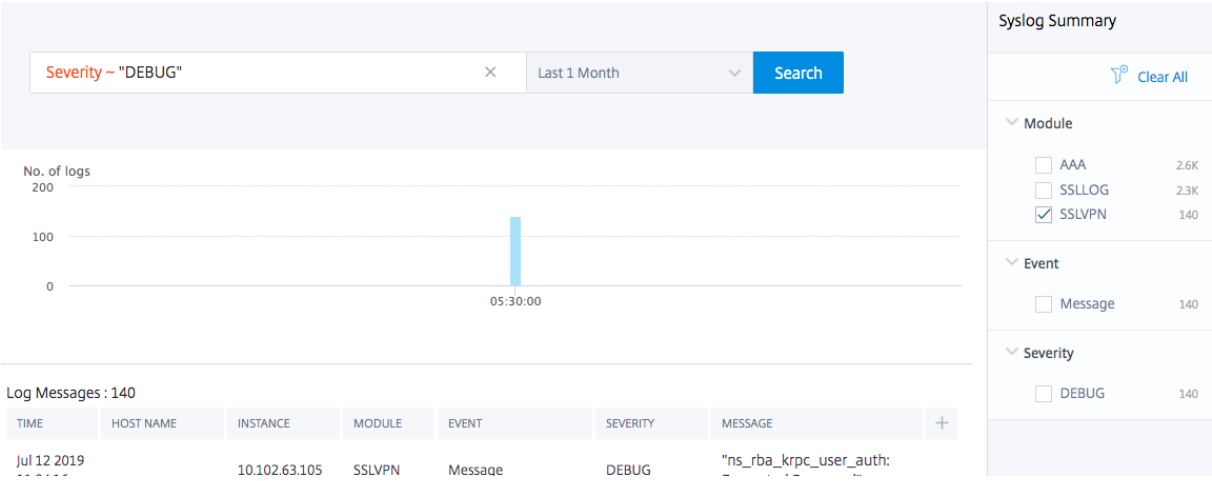
要搜索 NetScaler 控制台软件中存在的所有 NetScaler 控制台系统审核日志消息，请从 NetScaler 控制台 GUI 中导航到设置 **>** 审核日志消息。新的过滤器类别包括实例、模块、事件、严重性和消息。

要搜索 NetScaler 控制台中存在的所有应用程序的审核日志消息，请从 NetScaler 控制台 GUI 中导航到基础架构 **>** 网络功能 **>** 审核。

要在 NetScaler 控制台上搜索特定应用程序的审核日志消息，请从 NetScaler 控制台 GUI 中导航 到应用程序 控制面板，然后选择要搜索审核日志消息的虚拟服务器。接下来，单击 审核日志 选项卡。

选择筛选器类别后，指定它是否等于还是包含搜索词。

接下来，添加搜索词。对于某些类别，会显示预先填充的搜索词列表。默认情况下，搜索时间为 1 天。您可以通过单击向下箭头更改时间和日期范围。您可以从“**Syslog** 摘要”或“审核日志摘要”窗格中选择选项，进一步缩小搜索范围。

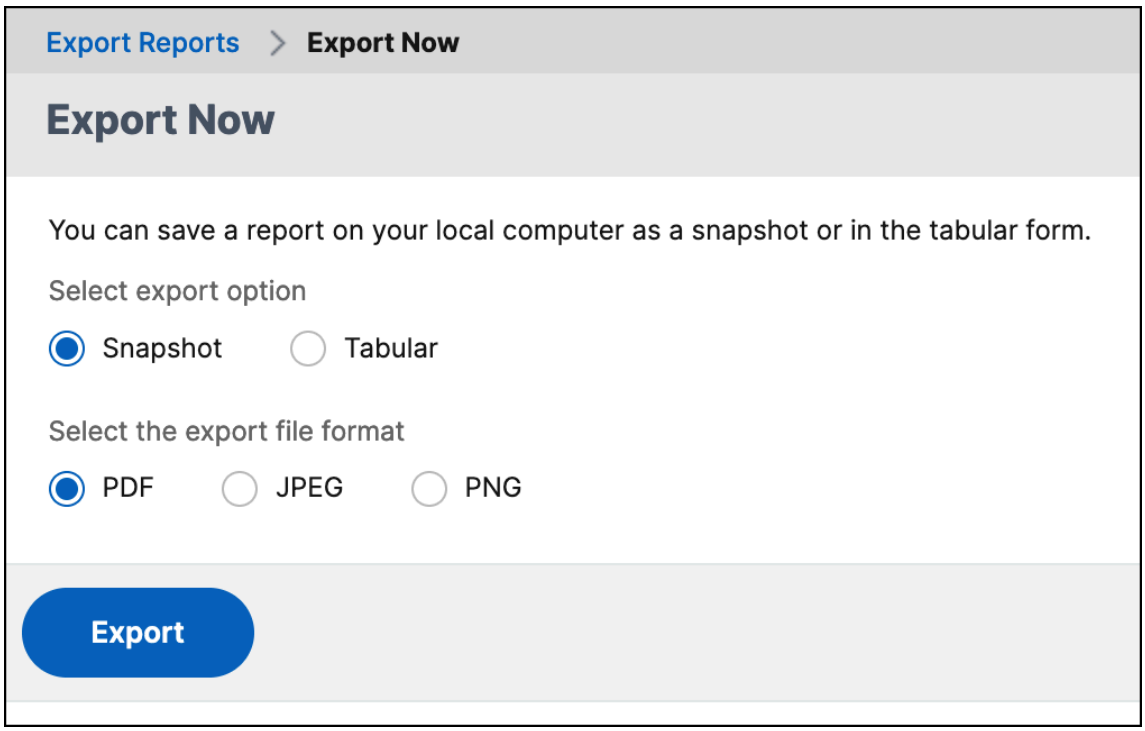


导出 **syslog** 消息

要使用 **NetScaler** 控制台导出系统日志消息报告，请执行以下操作：

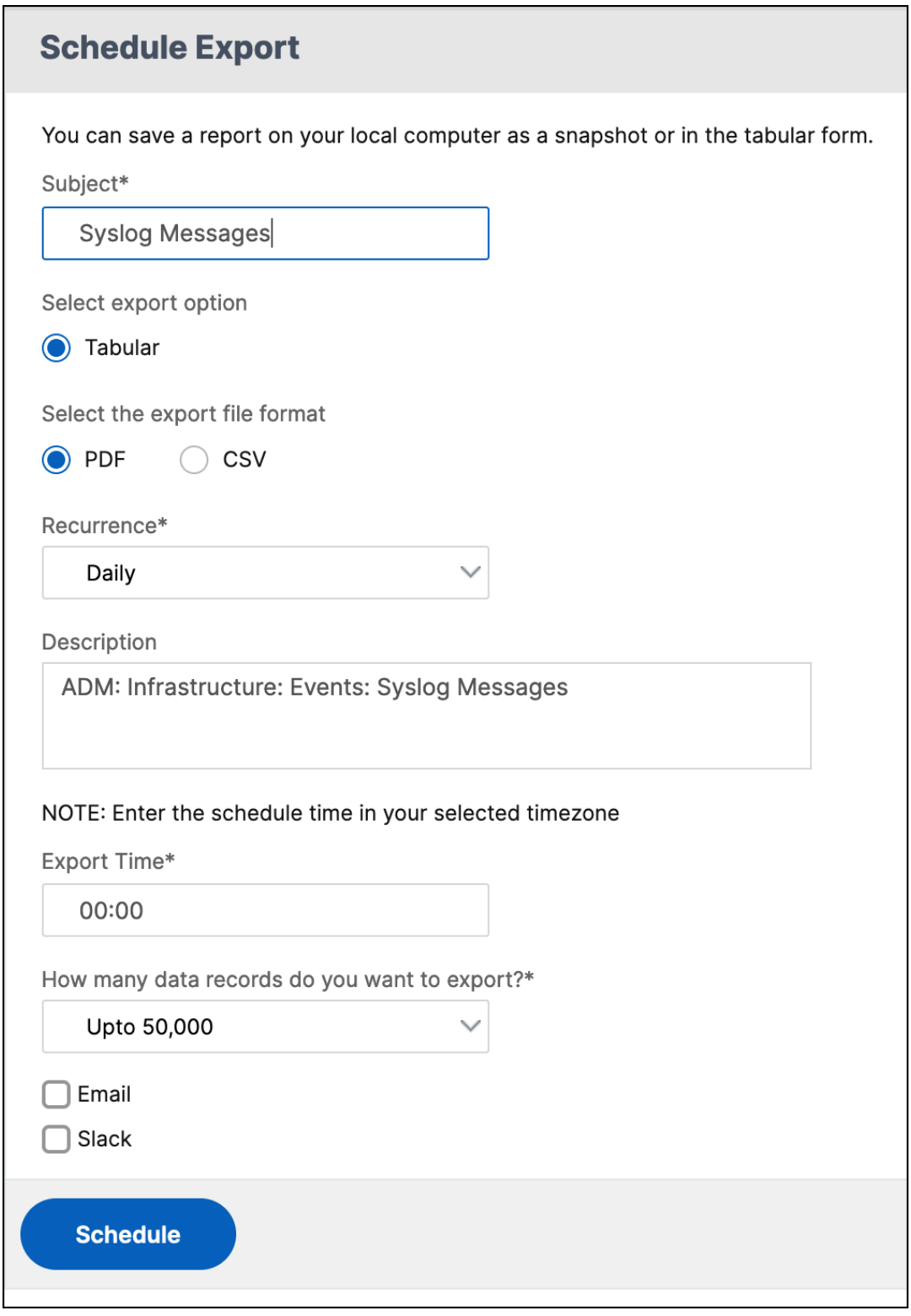
1. 导航到 基础结构 **>** 事件 **>** 系统日志消息。

2. 在右窗格中，单击“Syslog 消息”页右上角的导出按钮。
3. 在“立即导出”下，选择所需的格式，然后单击“导出”。



要使用 **NetScaler** 控制台安排系统日志消息报告的导出，请执行以下操作：

1. 导航到 基础结构 **>** 事件 **>** 系统日志消息。
2. 在 **Syslog** 消息 页面的右侧窗格中，单击“导出”。
3. 在计划报告选项卡下，设置以下参数：
    - 说明：描述导出报表原因的消息。
    - 格式：导出报告的格式。
    - 重复：导出报告的间隔。
    - 导出时间：导出报表的时间。按您的本地时区以 24 小时格式输入时间。
    - 电子邮件通讯组列表：通过电子邮件接收报告的收件人列表。从提供的列表中选择一个电子邮件分发列表。生成报告且满足计划的时间条件时触发电子邮件。如果要创建电子邮件通讯组列表，请单击 **+** 并提供邮件服务器和邮件配置文件详细信息。



禁止显示 **syslog** 消息

July 17, 2024

当配置为系统日志服务器时，NetScaler 控制台会接收来自已配置的 Citrix Application Delivery Controller (NetScaler) 实例的所有系统日志消息。可能有很多消息，您可能不想看到。例如，您可能对查看所有信息级消息不感兴趣。现在您可以丢弃其中一些您不感兴趣的 syslog 消息。您可以通过设置一些过滤器来抑制某些传入 NetScaler 控制台的系统日志消息。NetScaler 控制台会丢弃所有符合条件的消息。这些丢弃的消息不会出现在 NetScaler 控制台 GUI 上，这些消息也不会存储在客户的 NetScaler 控制台数据库中。

您可以通过设置一些过滤器来抑制传入 NetScaler 控制台的某些已记录的系统日志消息。用于阻止 syslog 消息的两个过滤器是严重性和设施。您还可以隐藏来自特定 NetScaler 实例或多个实例的消息。您还可以为 NetScaler 控制台提供文本模式来搜索和隐藏消息。NetScaler 控制台会丢弃所有符合条件的消息。这些丢弃的消息不会出现在 NetScaler 控制台 GUI 上，这些消息也不会存储在客户数据库中。因此，在存储服务器上节省了大量空间。

阻止 syslog 消息的一些用例如下：

- 如果您要忽略所有信息级别消息，则阻止级别 6（信息）
- 如果您仅要记录防火墙错误状况，则阻止级别 3（错误）以外的所有级别

通过创建筛选器禁止 **syslog** 消息

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 事件 **>** 系统日志消息。
2. 单击齿轮图标显示“抑制过滤器”页面。

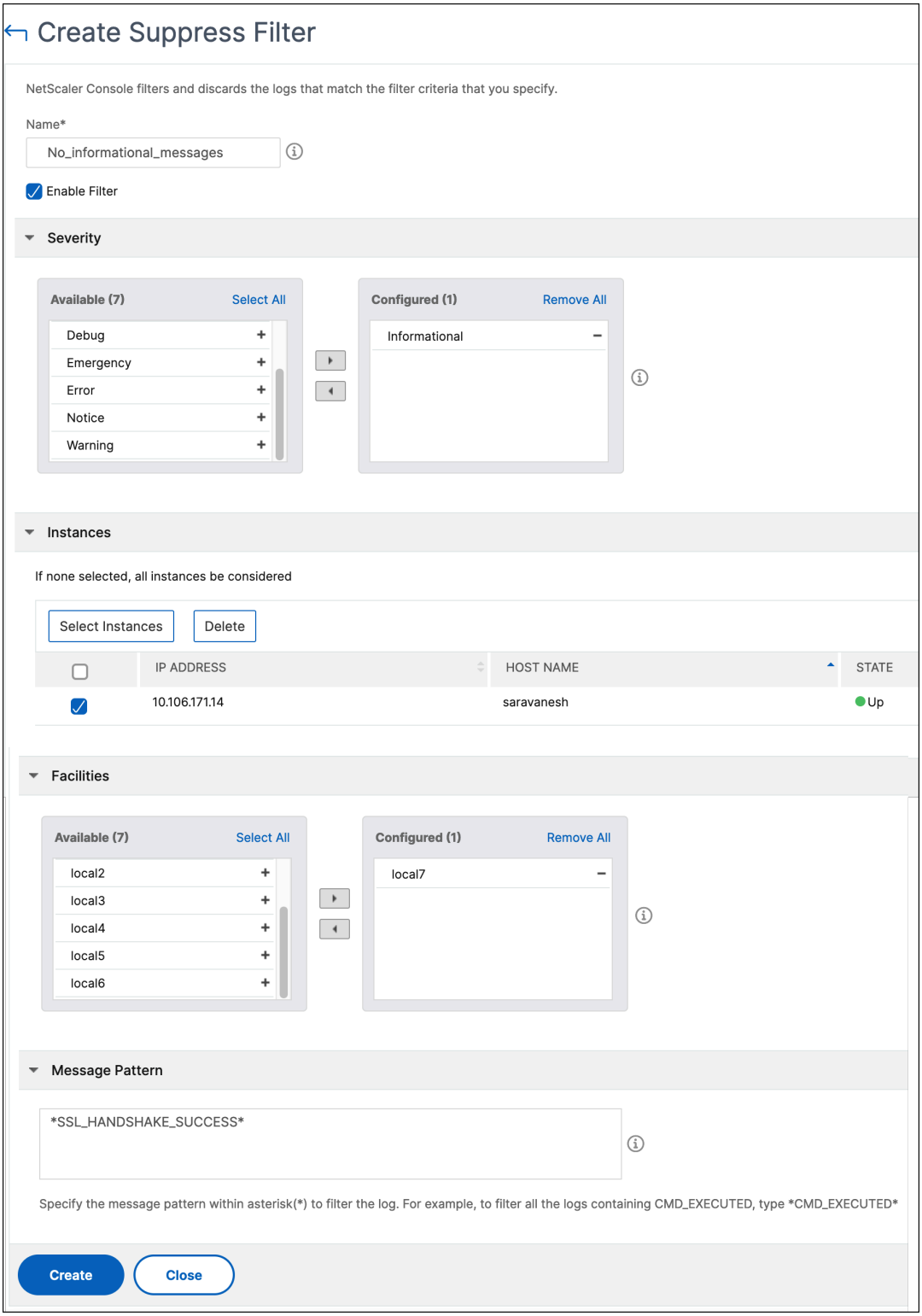
3. 在“禁止过滤器”页面中，单击“添加”。
4. 在“创建抑制过滤器”中，更新以下信息：

   a) 名称 -键入筛选器的名称。

   > 注意：
   >
   > 如果不同的用户对多个 NetScaler 实例具有不同的访问权限，则必须为不同的实例创建不同的筛选条件，因为用户只能看到他们有权访问所有实例的筛选条件。

   b) 严重性 -选择并添加必须隐藏消息的日志级别。
   例如，如果您不想查看传入的任何信息性消息，则可以选择“信息性”来隐藏这些消息。

   c) 实例 -选择已配置 syslog 消息的 NetScaler 实例。



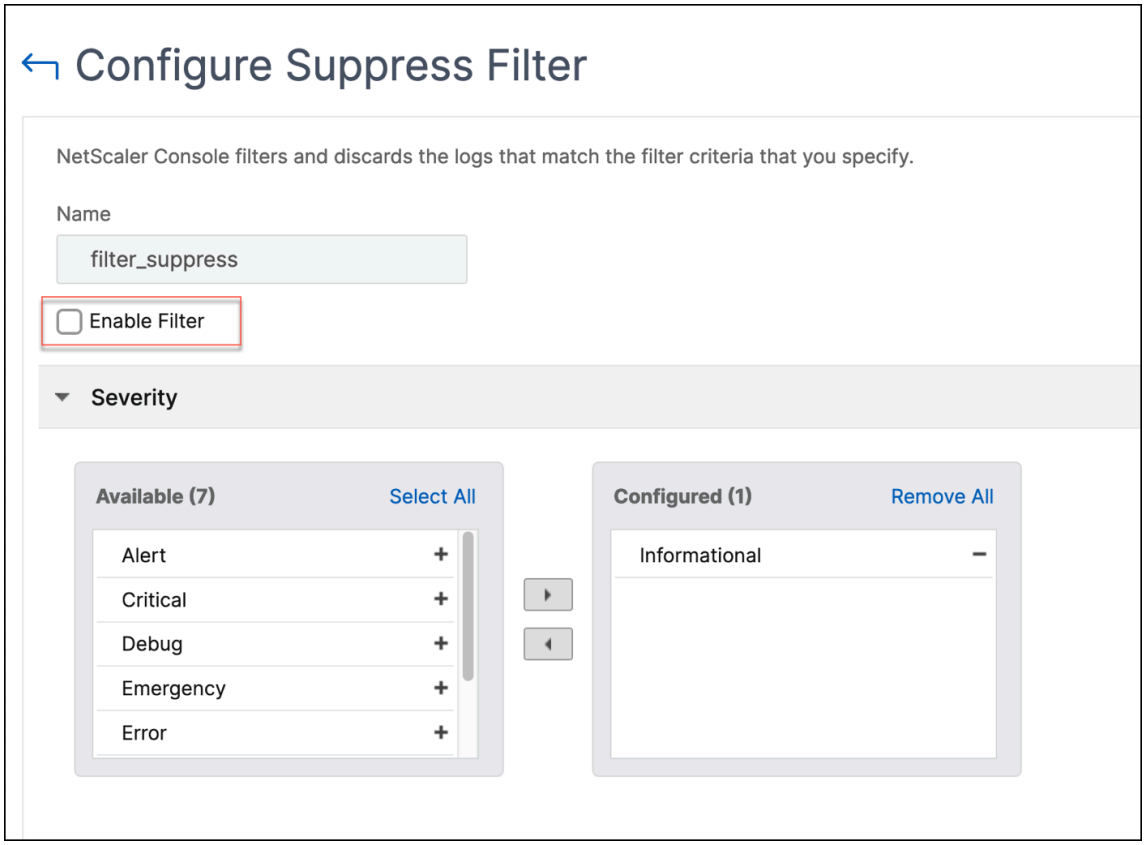
d) 设施 -根据生成消息的来源选择协作室以禁止消息。

e) 消息模式 -您还可以键入由星号 (*) 包围的文本模式来禁止消息。将在消息中搜索该文本模式字符串，并阻止包含此模式的那些消息。

禁用过滤器

要允许在 NetScaler 控制台上查看消息，必须禁用过滤器。

1. 导航到 基础结构 > 事件 > 系统日志消息。
2. 单击齿轮图标显示“抑制过滤器”页面。
3. 在“隐藏筛选器”页面中，选择过滤器并单击“编辑”。
4. 在“配置抑制筛选器”页面上，清除“启用筛选器”复选框以禁用筛选器。



SSL 控制板

May 9, 2024

NetScaler 控制台现在可以为您简化证书管理的各个方面。通过一个控制台可以建立自动化策略以确保合适的颁发者、密钥强度和正确的算法，同时密切跟踪未使用或即将过期的证书。要开始使用 NetScaler 控制台的 SSL 控制面板及其功能，您必须了解什么是 SSL 证书以及如何使用 NetScaler 控制台来跟踪您的 SSL 证书。

安全套接字层 (SSL) 证书是任何 SSL 事务的一部分，是标识公司（域）或个人的数字数据表单 (X509)。证书具有公钥组成部分，想要启动与服务器的安全事务的任何客户端都可以看见该组成部分。安全地驻留在 NetScaler 设备上的相

应私钥用于完成非对称密钥（或公钥）的加密和解密。

您可以通过以下任何一种方式获取 SSL 证书和密钥：

- 来自授权证书颁发机构 (CA)
- 通过在 NetScaler 设备上生成新的 SSL 证书和密钥

NetScaler 控制台提供安装在所有托管 NetScaler 实例上的 SSL 证书的集中视图。在 SSL 控制面板上，您可以查看有助于跟踪证书颁发者、密钥强度、签名算法、过期或未使用的证书等的图表。您还可以查看您的虚拟服务器上运行的 SSL 协议的分布情况以及这些服务器上启用的密钥。

您还可以设置通知，以便在证书即将过期时通知您，并包括有关哪些 NetScaler 实例使用这些证书的信息。

您可以将 NetScaler 实例证书关联到 CA 证书。但是，请确保您链接到同一 CA 证书的证书具有相同的来源和相同的颁发者。将一个或多个证书链接到 CA 证书后，可以取消它们的链接。

> 注意：
>
> 您还可以使用带有 NetScaler 控制台的 Venafi 信任保护平台服务器来自动管理 SSL 证书的整个生命周期。有关更多信息，请参阅自动 SSL 证书管理。

使用 **SSL** 控制板

May 9, 2024

您可以使用 NetScaler 控制台中的 SSL 证书控制面板查看图表，以帮助您跟踪证书颁发者、密钥优势和签名算法。SSL 证书控制板还显示指示以下信息的图形：

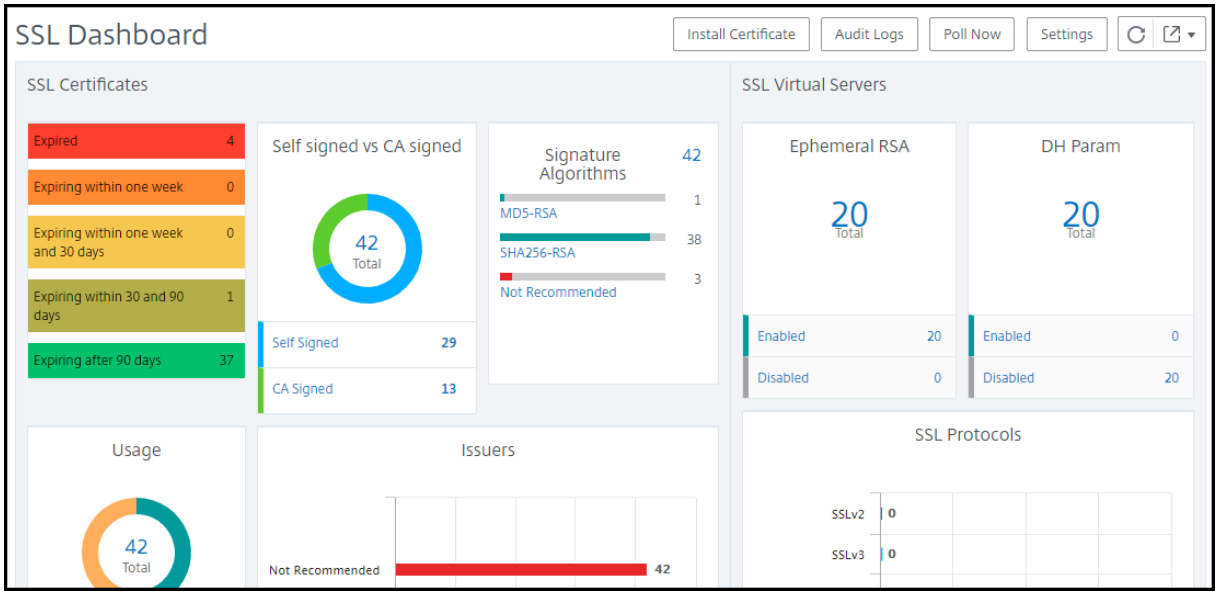
- 证书过期前的天数
- 已使用证书和未使用证书的数量
- 自签名证书和 CA 签名证书的数量
- 颁发者数
- 签名算法
- SSL 协议
- 按使用的证书数排在前 10 位的实例

监视 **SSL** 证书

如果贵公司的 SSL 策略中定义了特定的 SSL 证书要求，例如所有证书的最低密钥强度必须为 2048 位，并且必须由可信的 CA 机构授权，则使用 NetScaler 控制台上的 SSL 控制面板监视您的证书。

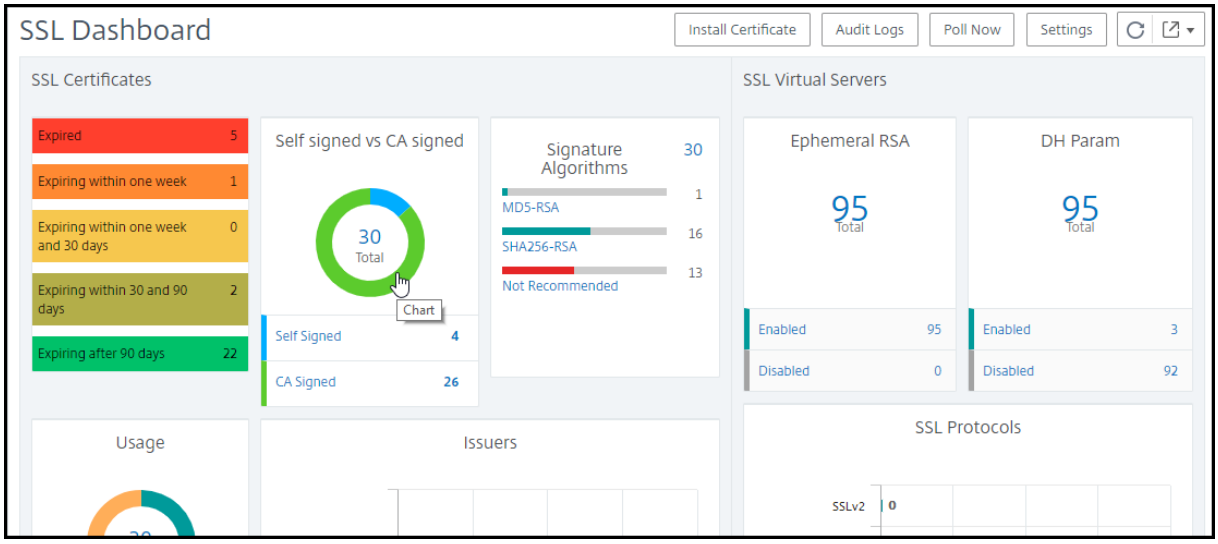
再例如，您可能上载了新证书，但忘记将其绑定到虚拟服务器。SSL 控制板会突出显示正在使用或未使用的 SSL 证书。在“使用情况”部分，您可以看到已安装的证书数以及正在使用的证书数。您可以进一步单击图表，查看证书名称、正在使用证书的实例、证书的有效性、签名算法等。

要在 NetScaler 控制台中监视 SSL 证书，请导航 到基础架构 **> SSL** 控制面板。

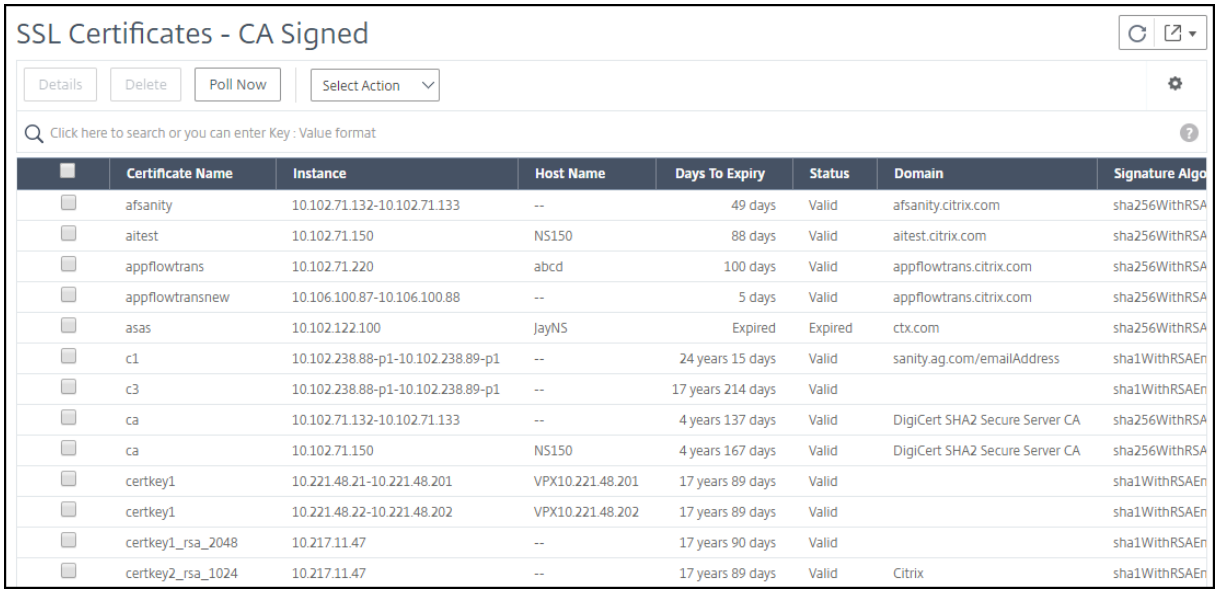


NetScaler 控制台允许您轮询 SSL 证书并将实例的所有 SSL 证书立即添加到 NetScaler 控制台。为此，请导航到 基础结构 **> SSL** 控制面板，然后单击 立即轮询。此时会弹出立即轮询页面，提供轮询网络中的所有 NetScaler 实例或轮询选定实例的选项。

您可以使用 NetScaler 控制台 SSL 控制面板来查看或监视 SSL 证书、SSL 虚拟服务器和 SSL 协议的详细信息。这些数字是超链接，您可以单击这些超链接来显示与 SSL 证书、SSL 虚拟服务器或 SSL 协议相关的详细信息。



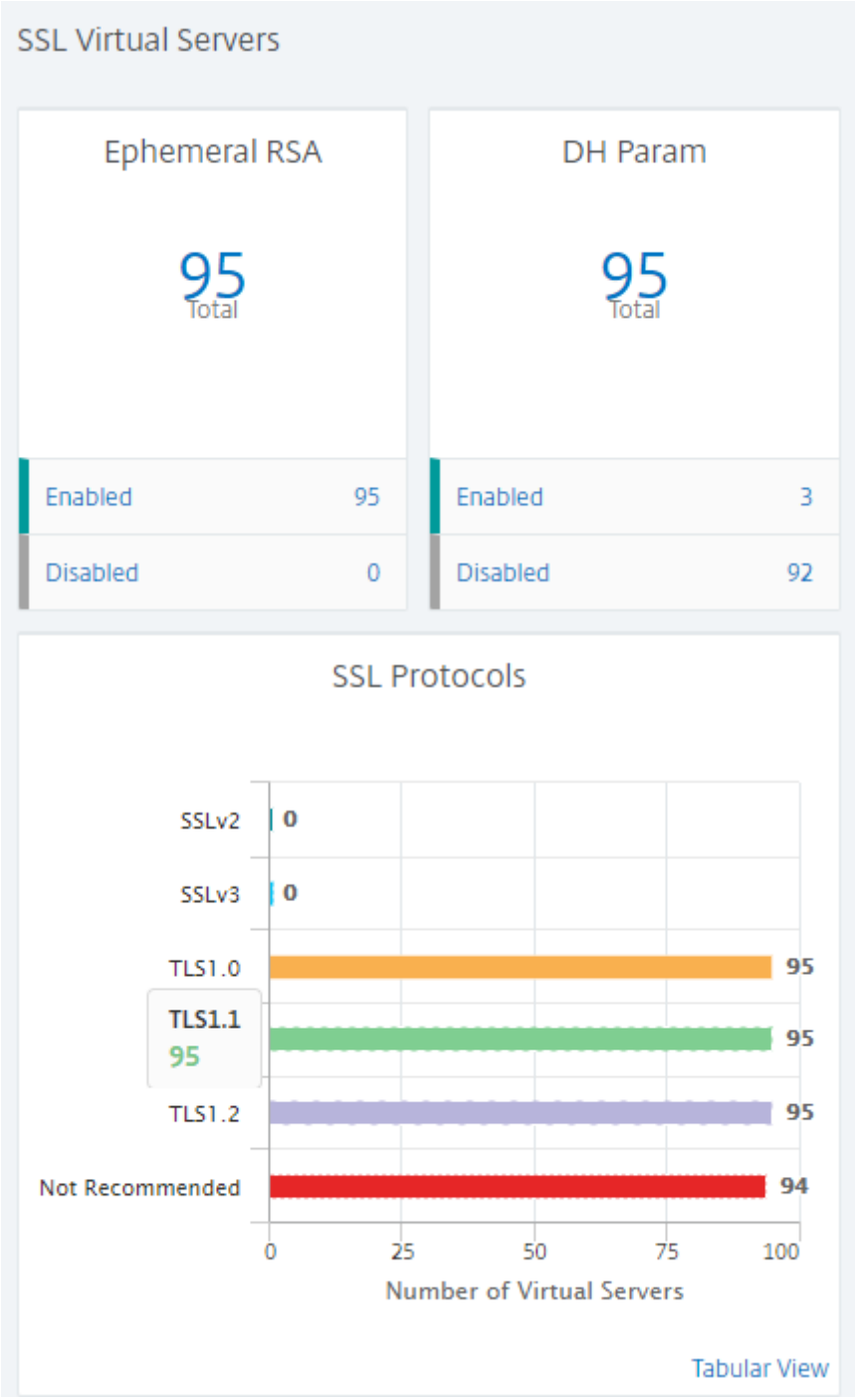
例如，当用户单击上图中的自签名与 **CA** 签名下的数字 30 时，将出现一个新窗口，显示了 NetScaler 实例上的 30 个 SSL 证书的详细信息。



Certificate Name	Instance	Host Name	Days To Expiry	Status	Domain	Signature Algo
afsanity	10.102.71.132-10.102.71.133	--	49 days	Valid	afsanity.citrix.com	sha256WithRSA
aitest	10.102.71.150	NS150	88 days	Valid	aitest.citrix.com	sha256WithRSA
appflowtrans	10.102.71.220	abcd	100 days	Valid	appflowtrans.citrix.com	sha256WithRSA
appflowtransnew	10.106.100.87-10.106.100.88	--	5 days	Valid	appflowtrans.citrix.com	sha256WithRSA
asas	10.102.122.100	JayNS	Expired	Expired	ctx.com	sha256WithRSA
c1	10.102.238.88-p1-10.102.238.89-p1	--	24 years 15 days	Valid	sanity.ag.com/emailAddress	sha1WithRSAEn
c3	10.102.238.88-p1-10.102.238.89-p1	--	17 years 214 days	Valid		sha1WithRSAEn
ca	10.102.71.132-10.102.71.133	--	4 years 137 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
ca	10.102.71.150	NS150	4 years 167 days	Valid	DigiCert SHA2 Secure Server CA	sha256WithRSA
certkey1	10.221.48.21-10.221.48.201	VPX10.221.48.201	17 years 89 days	Valid		sha1WithRSAEn
certkey1	10.221.48.22-10.221.48.202	VPX10.221.48.202	17 years 89 days	Valid		sha1WithRSAEn
certkey1_rsa_2048	10.217.11.47	--	17 years 90 days	Valid		sha1WithRSAEn
certkey2_rsa_1024	10.217.11.47	--	17 years 89 days	Valid	Citrix	sha1WithRSAEn

NetScaler 控制台 SSL 控制面板还显示在您的虚拟服务器上运行的 SSL 协议的分布情况。作为管理员，您可以指定要通过 SSL 策略监视的协议，有关详细信息，请参阅 配置 SSL 策略。支持的协议为 SSLv2、SSLv3、TLS1.0、TLS1.1 和 TLS1.2。虚拟服务器上使用的 SSL 协议以条形图格式显示。单击特定协议会显示使用该协议的虚拟服务器列表。

在 SSL 控制板上启用或禁用 Diffie-Hellman (DH) 或 Ephemeral RSA 密钥后，将显示圆环图。即使服务器证书不支持导出客户端，使用这些密钥也可以与导出客户端进行安全通信，就像使用 1024 位证书一样。单击相应的图表将显示启用 DH 或临时 RSA 密钥的虚拟服务器的列表。



查看 **SSL** 证书的审核日志

现在，您可以在 NetScaler 控制台上查看 SSL 证书的日志详情。日志详细信息显示在 NetScaler 控制台上使用 SSL 证书执行的操作，例如：安装 SSL 证书、链接和取消链接 SSL 证书、更新 SSL 证书以及删除 SSL 证书。在监视具有多个所有者的应用程序上进行的 SSL 证书更改时，审核日志信息很有用。

要查看使用 SSL 证书在 NetScaler 控制台上执行的特定操作的审核日志，请导航到基础架构 **> SSL** 控制板，然后选择审核日志。

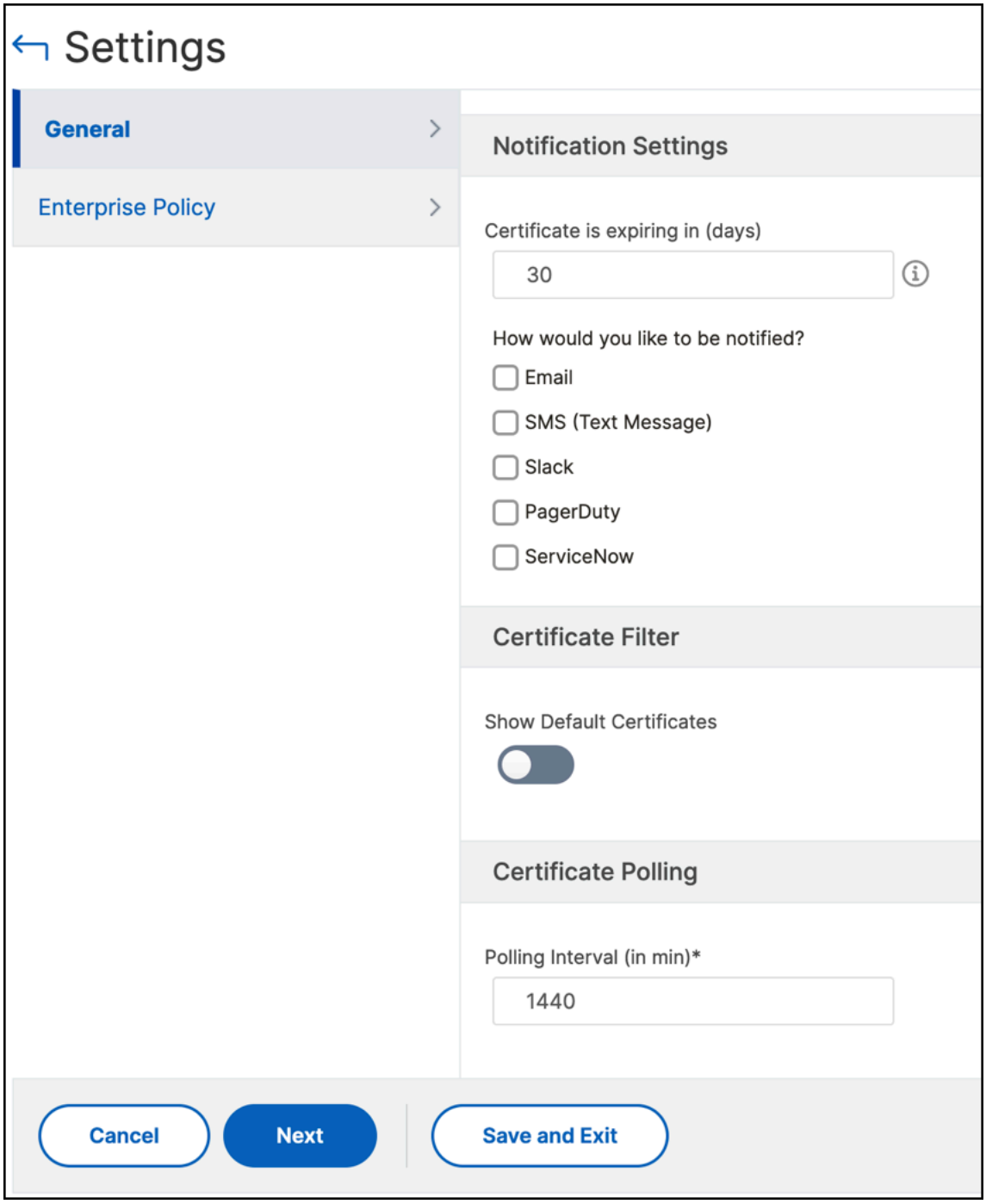
对于使用 SSL 证书执行的特定操作，您可以查看其状态、开始时间和结束时间。此外，您可以查看在其上执行操作的实例以及在该实例上运行的命令。

排除 **SSL** 控制板上的默认 **NetScaler** 证书

NetScaler 控制台允许您根据自己的喜好显示或隐藏 SSL 控制面板图表上显示的默身份验证书。默认情况下，所有证书（包括默身份验证书）都显示在 SSL 控制面板上。

要在 **SSL** 控制板上显示或隐藏默身份验证书，请执行以下操作：

1. 在 NetScaler 控制台 GUI 中导航到基础架构 **> SSL** 控制面板。
2. 在“**SSL** 控制板”页面上，单击“设置”。
3. 在设置页面上，选择 常规。
4. 在证书过滤器部分，禁用显示默身份验证书，然后选择保存并退出。



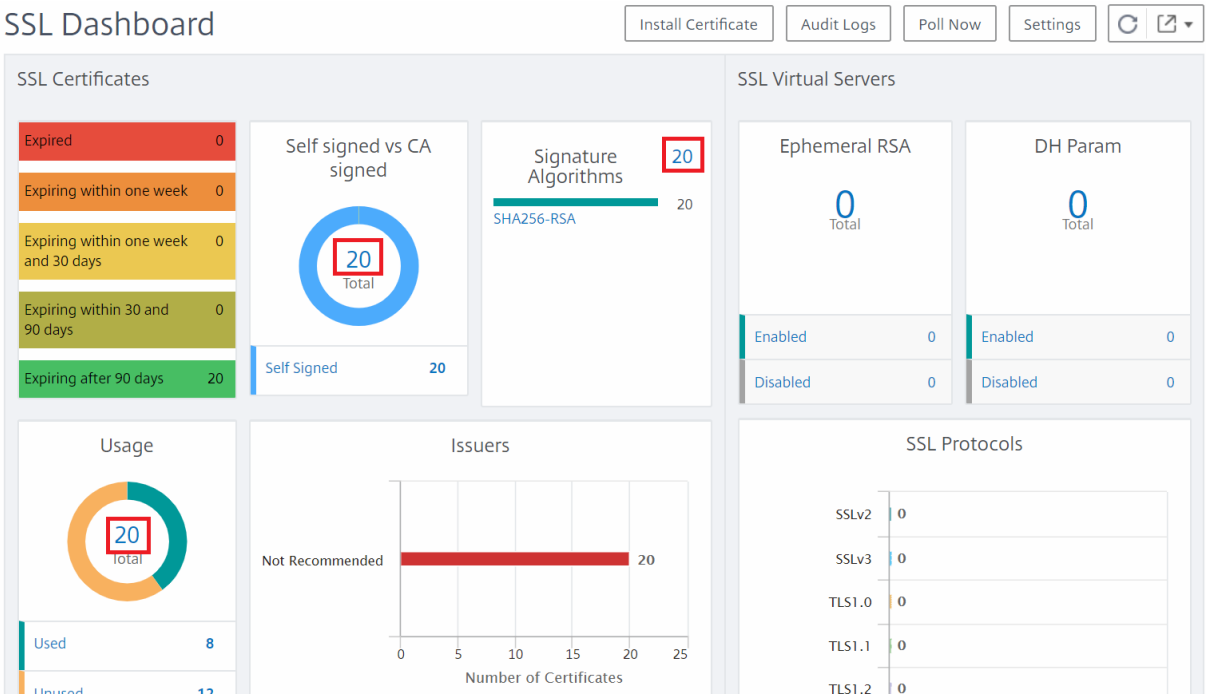
下载 **SSL** 证书

SSL 证书必须按实例单独管理。NetScaler 控制台让您可以查看在多个实例上部署的所有证书。

- 您可以选择哪些证书即将到期并自动续订证书。
- 可以围绕允许的证书类型和签名颁发机构来设置和强制执行策略。
- 您也可以下载 SSL 证书进行续订，然后再上载。

要下载 **SSL** 证书，请：

1. 在 NetScaler 控制台 GUI 中导航到基础架构 **> SSL** 控制面板。
2. 在 **SSL** 控制面板 页面上，单击任何图表中的 SSL 证书总数。



1. 在 **SSL** 证书页面上，单击要下载的证书。例如，您想下载将在未来一周内到期的版本。
2. 从“选择操作”列表框中，选择“下载”。
   证书将下载到您的系统。

要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

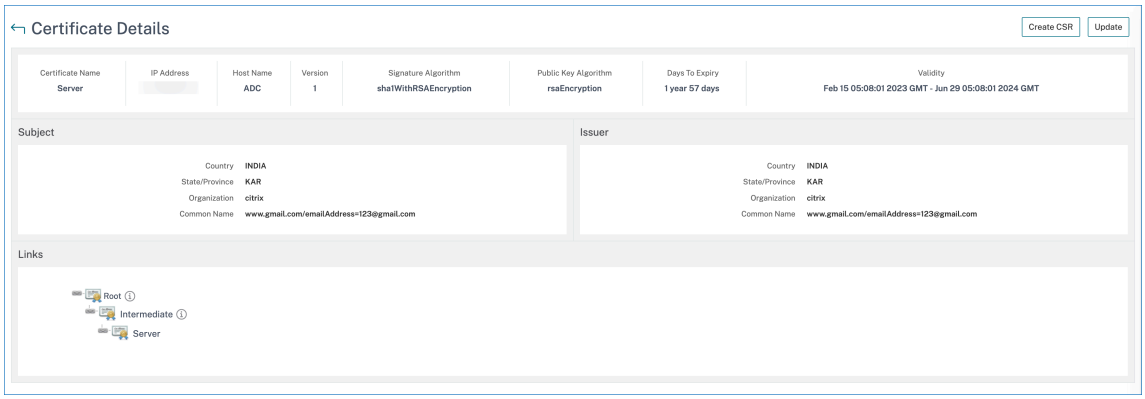
> 注意
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

查看 **SSL** 证书链

您可以查看证书的完整链接链，包括中间证书直至根 CA 证书。

要查看证书链，请执行以下操作：

1. 导航到基础架构 **> SSL** 控制面板，然后在任意图块中单击 SSL 证书。
2. 在 **SSL** 证书页面中，选择证书并单击详细信息。证书链显示在“链接”下。



设置 SSL 证书过期通知

May 9, 2024

作为安全管理员，您可以在证书即将到期时配置通知，并添加有关哪些 NetScaler 实例使用这些证书的信息。通过启用通知，您可以及时续订您的 SSL 证书。

例如，您可以设置在您的证书即将过期前的 30 天向电子邮件通讯组列表发送电子邮件通知。

要设置来自 **NetScaler** 控制台的通知，请执行以下操作：

1. 在 NetScaler 控制台中，导航到基础架构 **> SSL** 控制面板。
2. 在 **SSL** 控制面板 页面上，单击 设置。
3. 在“设置”页面上，单击“常规”。
4. 在“通知设置”部分中，根据到期日期之前的天数指定何时发送通知。
5. 选择要发送的通知类型。从菜单中选择通知类型和分发列表。通知类型如下：
   - **Email**（电子邮件）- 指定邮件服务器和配置文件详细信息。证书要过期时将触发电子邮件。
   - **Slack** -指定松弛配置文件。当您的证书即将到期时，系统会发送通知。
   - **PagerDuty** -指定 PagerDuty 配置文件。根据在 PagerDuty 门户中配置的通知设置，当证书即将过期时，系统会发送通知。
   - **ServiceNow** -当您的证书即将过期时，会向默认的 ServiceNow 配置文件发送通知。

     > 重要
     >
     > 须确保 Citrix Cloud ITSM Adapter 已为 ServiceNow 配置并与 NetScaler 控制台集成。有关

> 更多信息，请参见 将 NetScaler 控制台与 ServiceNow 实例集成。

6. 点击 保存并退出。

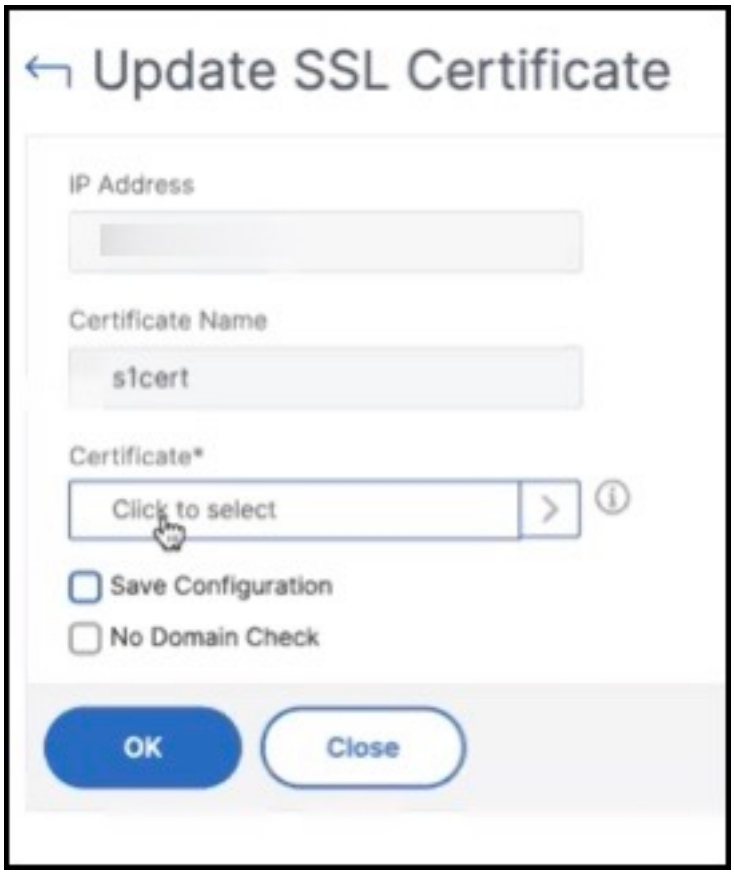
更新已安装的证书

January 29, 2024

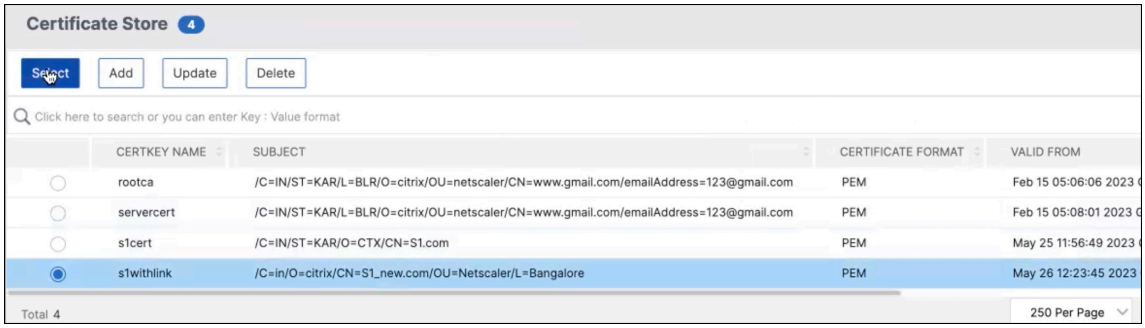
收到证书颁发机构 (CA) 的续订证书后，您无需登录单个 NetScaler 实例即可更新证书。您可以使用证书存储库中的证书更新 NetScaler 控制台中的现有证书。

要从 NetScaler 控制台更新 SSL 证书，请执行以下操作：

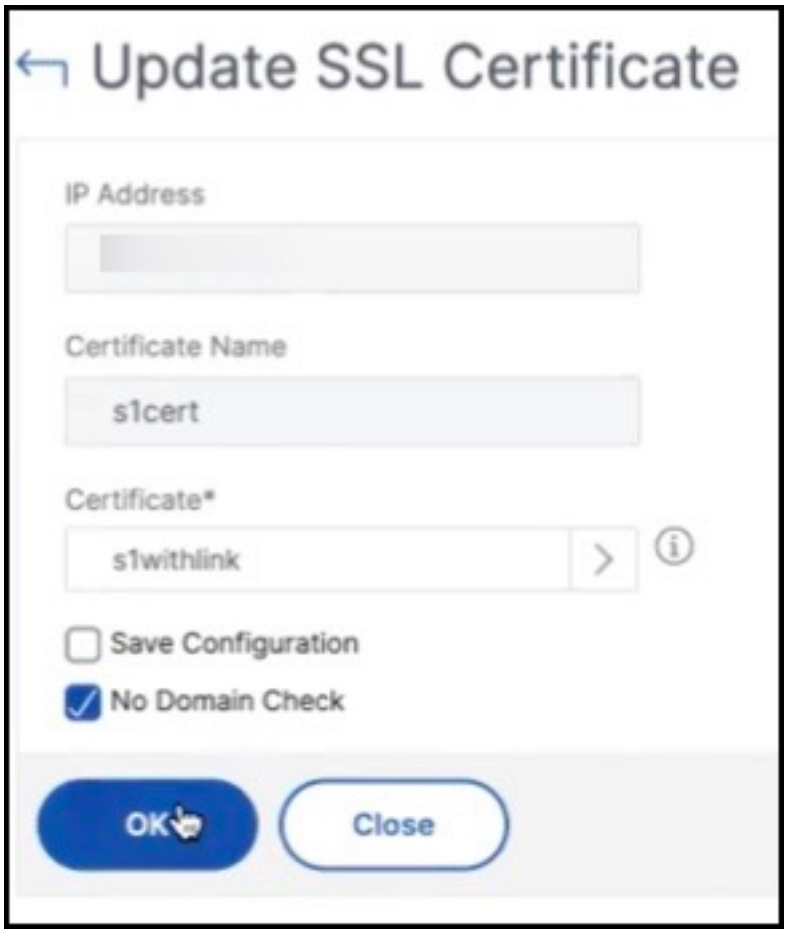
1. 在 NetScaler 控制台中，导航 到基础架构 **> SSL** 控制面板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 在 **SSL** 证书 页面中，选择证书并单击 更新。或者，单击 SSL 证书以查看其详细信息，然后单击 **SSL** 证书 页面右上角的 更新。
4. 在 更新 **SSL** 证书 页面中，选择 证书 以显示 证书存储 页面。



5. 在“证书存储”页面中，选择要添加的证书文件。单击 **Select**（选择）。

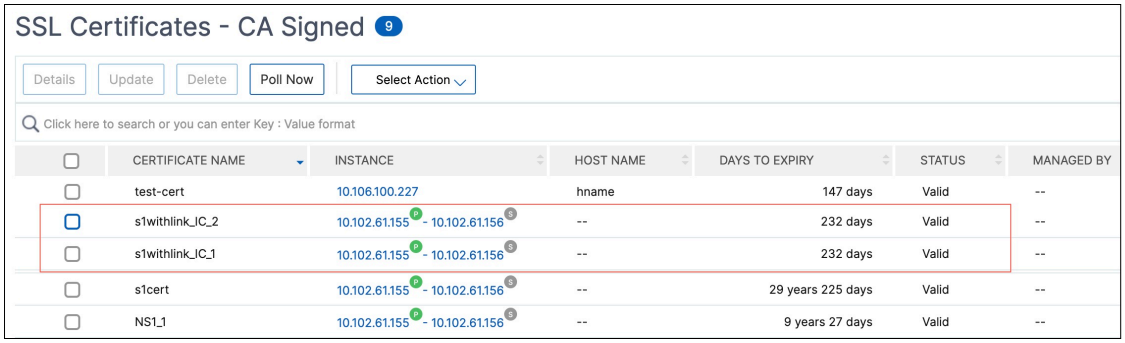


6. 如果新证书的域名与旧证书不匹配，并且您希望服务器托管新域，请选择 不进行域名检查。

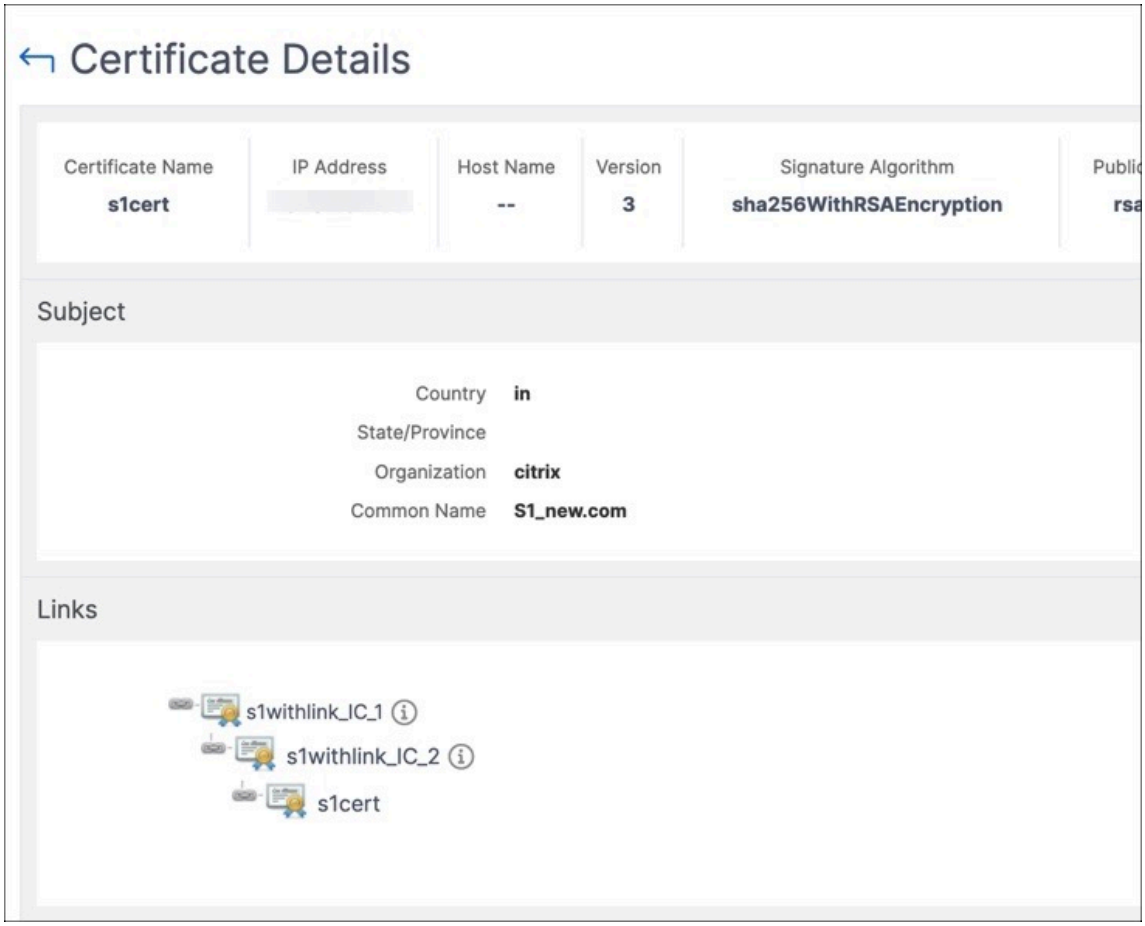


单击确定。此证书绑定到的所有 SSL 虚拟服务器都会自动更新。

当您使用证书存储中的证书链更新现有 SSL 证书时，现有证书将使用链接的证书进行更新。



选择证书并单击“详细信息”以查看证书链。



在 **NetScaler** 实例上安装 **SSL** 证书

May 9, 2024

在 NetScaler 实例上安装 SSL 证书之前，请确保证书由受信任的 CA 颁发。此外，请确保证书密钥的密钥强度为 2,048 位或更高，并且密钥使用安全签名算法进行签名。

要从另一个 **NetScaler** 实例安装 **SSL** 证书，请执行以下操作：

您还可以从选定的 NetScaler 实例导入证书，然后从 NetScaler 控制台 GUI 将其应用于其他目标 NetScaler 实例。

1. 导航到基础结构 **> SSL** 控制面板。
2. 在 SSL 控制板的右上角，单击 安装。
3. 在 **NetScaler** 实例上安装 **SSL** 证书 页面上，指定以下参数：

   a) 证书来源

   选择“从实例导入”选项。

   - 选择要从中导入证书的 实例。
   - 从实例上所有 SSL 证 书文件的列表中选择证书。

   b) 证书详情

   - 证书名称。指定证书密钥的名称。
   - 密码。用于加密私钥的密码。可以使用此选项上载加密的私钥。

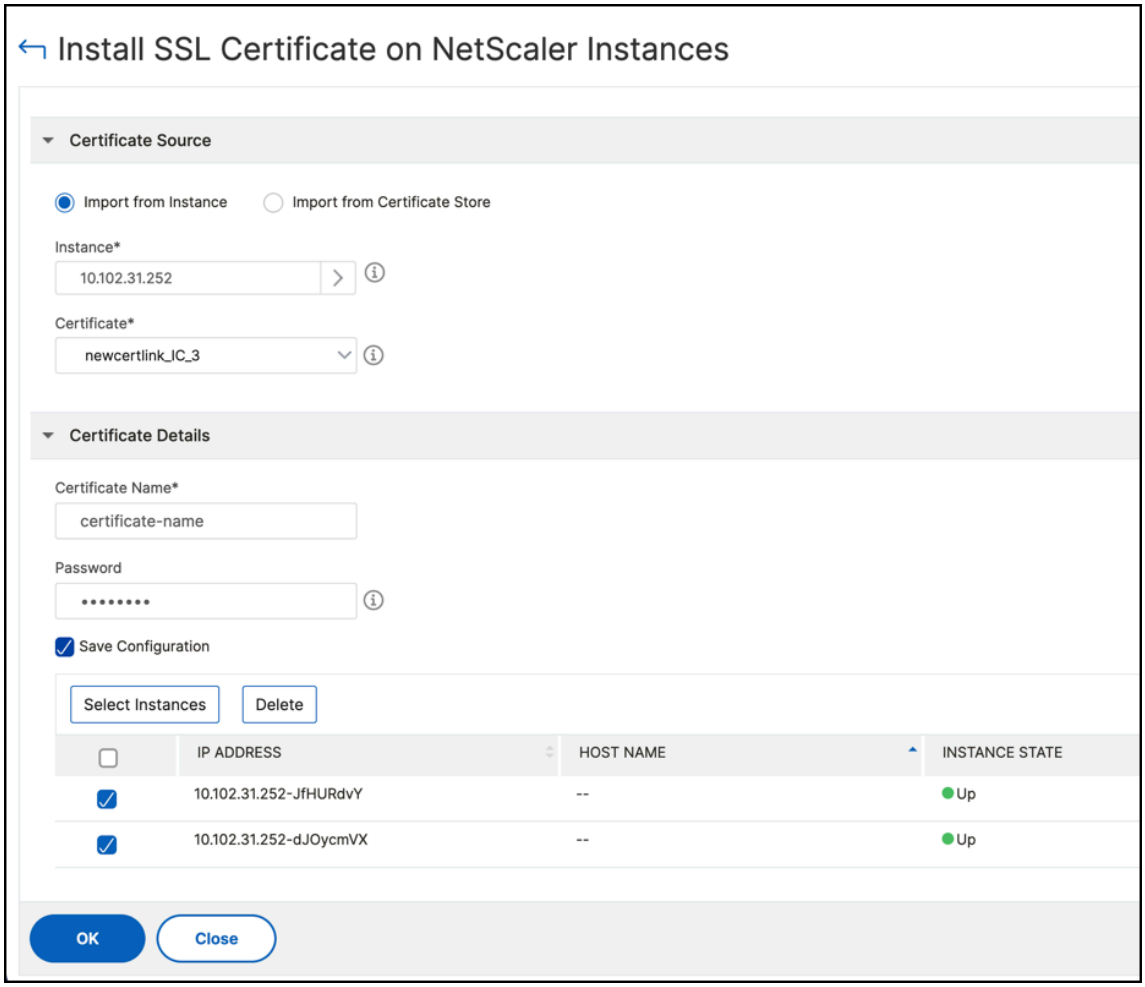
4. 单击“选择实例”以选择要安装证书的 NetScaler 实例。
5. 单击“确定”。

要从 **NetScaler** 控制台安装 **SSL** 证书，请执行以下操作：

1. 导航到基础结构 **> SSL** 控制面板。
2. 在控制面板的右上角，单击“安装证书”。
3. 在在 **NetScaler** 实例上安装 **SSL** 证书页面上，指定以下参数：

   - 证书文件 -通过选择本 地（您的本地 计算机）或 设备（证书文件必须存在于 NetScaler 实例上）上载 SSL 证书文件。
   - **Key File**（密钥文件）- 上载密钥文件。
   - **Certificate Name**（证书名称）–指定证书密钥的名称。
   - **Password**（密码）- 用于对私钥进行加密的密码。可以使用此选项上载加密的私钥。
   - 选择实例 -选择要安装证书的 NetScaler 实例。

4. 要保存配置以备将来使用，请选中“保存配置”复选框。
5. 单击确定。



创建证书签名请求 (CSR)

May 9, 2024

证书签名请求 (CSR) 是将在其中使用证书的服务器上生成的加密文本块。它包含证书中包含的信息，例如组织名称、公用名称（域名）、地点和国家/地区。

要使用 **NetScaler** 控制台创建 **CSR**，请执行以下操作：

1. 在 NetScaler 控制台中，导航到基础架构 **> SSL** 控制面板。
2. 单击任意图表以查看已安装 SSL 证书的列表，然后选择要为其创建 CSR 的证书，然后从选择操作下拉列表中选择创建 **CSR**。
3. 在 **Create Certificate Signing Request (CSR)**（创建证书签名请求 (CSR)）页面上，为 CSR 指定名称。
4. 执行以下操作之一：

- **Upload a key**（上载密钥）- 选择 **I have a Key**（我有密钥）选项。要上载密钥文件，请选择本地（您的本地 计算机）或设备（密钥文件必须存在于 NetScaler 控制台虚拟实例上）。
- 创建密钥 - 选择“我没有密钥”选项，然后指定以下参数：

加密算法	Type of key（密钥类型）。例如 RSA。
Key File Name（密钥文件名称）	存储 RSA 密钥的文件的名称。
密钥大小	密钥大小（以位为单位）。
Public Exponent Value（公共指数值）	从提供的下拉列表中选择 **3** 或 **F4** 。此值属于创建 RSA 密钥所需的密码算法的一部分。
Key Format（密钥格式）	默认情况下，选择 PEM。PEM 是建议的 SSL 证书密钥格式。
PEM Encoding Algorithm（**PEM** 编码算法）	在下拉列表中，选择要用于加密生成的 RSA 密钥的算法（**DES** 或 **DES3**）。如果选择此算法，则必须提供 PEM 密码短语。
PEM Passphrase（**PEM** 密码）	如果您选择了 PEM 编码算法，请输入密码。
Confirm PEM Passphrase（确认 **PEM** 密码）	确认 PEM 密码。

5. 单击继续。
6. 在下一页中，提供更多详细信息。

   大多数字段都有从所选证书的主题提取的默认值。主题包含公用名、组织名称、省/市/自治区和国家/地区之类的详细信息。

   在“主 题备用名称”字段中，您可以使用单个证书指定多个值，例如域名和 IP 地址。主题备选名称可帮助您使用单个证书保护多个域的安全。

   按以下格式指定域名和 IP 地址：

   ```
   DNS:<Domain name>, IP:<IP address>
   ```

   在这个例子中，它可以保护 `10.0.0.1` 和 `www.example.com`。

   查看字段，然后单击 继续。

> 注意
>
> 大多数 CA 接受通过电子邮件提交证书。CA 将向您提交 CSR 的电子邮件地址返回有效证书。

链接和取消链接 **SSL** 证书

January 29, 2024

可以将多个证书链接在一起来创建证书捆绑包。要将证书链接到另一个证书，第一个证书的颁发者必须匹配第二个证书的域。例如，如果要将证书 A 链接到证书 B，则证书 A 的“颁发者”必须与证书 B 的“域”相匹配。

要使用 **NetScaler** 控制台将一个 **SSL** 证书链接到另一个证书，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **> SSL** 控制面板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 选择要关联的证书，然后从“选择 操作”下拉列表中选择“链接”。
4. 从匹配的证书列表中选择要链接到的证书，然后单击 **OK**（确定）。

> 注意
>
> 如果未找到匹配的证书，将显示以下消息：No certificate found to link（未找到证书进行链接）。

要使用 **NetScaler** 控制台取消关联 **SSL** 证书，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **> SSL** 控制面板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 选择任一关联证书，然后从“选择 操作”下拉列表中选择“取消链接”。
4. 单击确定。

> 注意
>
> 如果所选证书未链接到另一个证书，将显示以下消息：Certificate does not have any CA link（证书没有任何 CA 链接）。

配置企业策略

August 8, 2024

您可以配置企业策略，添加所有可信的 CA、安全签名算法，并在 NetScaler 控制台中为证书密钥选择推荐的密钥强度。如果您的 NetScaler 实例上安装的任何证书尚未添加到企业策略中，则 SSL 证书控制板会将这些证书的颁发者显示为“不推荐”。

此外，如果证书密钥强度与企业策略中的推荐密钥强度不一致，SSL 证书控制板上那些密钥的强度将显示为“Not Recommended”（不推荐）。

要在 **NetScaler** 控制台上配置企业策略，请执行以下操作：

1. 在 NetScaler 控制台中，导航到基础架构 **> SSL** 控制面板，然后单击“设置”。
2. 在设置页面上，单击企业策略图标添加所有可信 CA、保护签名算法，然后为证书和密钥选择推荐的密钥强度。支持的密钥强度为 512、1024、2048、3072 和 4096 位。
    - 推荐的关键优势 -表示算法安全性和密钥中的位数。
    - 推荐的签名算法 -表示应用程序的签名令牌问题。
    - 推荐的可信 **CA** -表示颁发数字证书的可信实体。单击 **+** 图标可添加更多实体。
    - 推荐的 **SSL** 协议 - 表示 TLS/SSL 版本。
3. 单击完成或保存并退出以保存企业策略。

> 注意
>
> SSL 控制板仅显示通过“设置”选项选择的“签名算法”，其他则显示为“不推荐”。

轮询 **NetScaler** 实例中的 **SSL** 证书

May 9, 2024

NetScaler 控制台使用 NITRO 调用和安全复制 (SCP) 协议每隔 24 小时自动轮询一次 SSL 证书。您还可以手动轮询 SSL 证书，以发现 NetScaler 实例上新添加的 SSL 证书。轮询所有 NetScaler 实例 SSL 证书会给网络带来沉重负载。

您可以仅手动轮询一个或多个选定实例的 SSL 证书，而不是轮询所有 NetScaler 实例 SSL 证书。

要在 **NetScaler** 实例上轮询 **SSL** 证书，请执行以下操作：

1. 导航到基础结构 **> SSL** 控制面板。
2. 在 **SSL** 控制板页面的右上角，单击立即轮询。
3. 此时会弹出立即轮询页面，您可以选择轮询网络中的所有 NetScaler 实例或轮询选定实例。
    a) 要轮询所有 NetScaler 实例的 SLL 证书，请选择所有实例选项卡，然后单击开始轮询。
4. 要轮询特定实例，请选择“选择实例”选项卡，从列表中选择实例，然后单击“立即轮询”。

使用 **NetScaler** 控制台证书存储区管理 **SSL** 证书

June 7, 2024

NetScaler 控制台证书存储可帮助您在一个位置存储和管理 SSL 证书。以后，您可以使用存储的证书来配置 NetScaler 设置。

证书存储允许您添加、更新和删除 SSL 证书。您还可以使用证书存储从 NetScaler 实例导入证书，然后将其应用于其他目标 NetScaler 实例。

将 **SSL** 证书添加到证书存储区

1. 导航到基础结构 **>** **SSL** 控制面板 **>** 证书存储。单击添加。
2. 在 添加证书 页面上，输入以下详细信息：
    - 证书密钥名称 -输入证书的名称。名称必须只有 ASCII 字母数字、下划线和连字符字符，并且必须少于 30 个字符。证书创建后不能更改名称。
    - 证书文件 -浏览到您的本地驱动器并上载证书文件。
    - 密钥文件 -从本地计算机上载密钥文件。
    - 密码 -如果您有 PEM 格式的加密私钥，请键入用于加密私钥的密码。
    - 添加证书链 -选择此选项可将证书添加到证书链中。
    - 证书链 -浏览到您的本地驱动器并上载证书文件。
    - 单击创建。

更新证书存储区中的 **SSL** 证书

1. 导航到基础结构 **>** **SSL** 控制面板 **>** 证书存储。选择要更新的证书，然后单击“更新”。
2. 在 更新证书 页面上，输入以下详细信息：
    - **Certkey** 名称 -显示您选择要更新的证书的名称。
    - 证书文件 -要更新证书文件，请上载证书文件。
    - 密钥文件 -要更新密钥文件，请从本地计算机上载密钥文件。
    - 密码 -如果您有 PEM 格式的加密私钥，请键入用于加密私钥的密码。
    - 添加证书链 -选择此选项可将证书添加到证书链中。
    - 证书链 -浏览到您的本地驱动器并上载证书文件。
    - 单击确定。

从证书存储中删除 **SSL** 证书

1. 导航到基础结构 **>** **SSL** 控制面板 **>** 证书存储。单击删除。
2. 出现提示时，单击“是”删除证书。

在 **NetScaler** 实例上安装 **SSL** 证书

1. 导航到基础结构 **>** **SSL** 控制面板 **>** 证书存储。选择要在 NetScaler 实例上安装的证书。
2. 在 **NetScaler** 实例上安装 **SSL** 证书 页面中，输入以下详细信息：

   a。证书来源

   - 证书 -显示所选证书的名称。

   b. 证书详情

   - 证书名称 -显示证书的名称。
   - 保存配置 -选择此选项可保存 NetScaler 配置。NetScaler 配置将在安装证书后保存。
3. 单击“选择实例”以选择要安装证书的 NetScaler 实例。

单击确定。

从 **NetScaler** 实例导入证书

1. 导航到基础结构 **>** **SSL** 控制面板 **>** 证书存储。单击“导入 **NetScaler** 证书”。
2. 在“导入 **NetScaler** 证书”页面中，您可以选择以下选项卡之一：

   - 导入 **NetScaler** 证书 - 单击“开始轮询”以轮询所有 NetScaler 实例上的所有 SSL 证书。
   - 选择实例 - 选择 NetScaler 实例，然后单击“导入 **NetScaler** 证书”，仅轮询所选 NetScaler 实例上的 SSL 证书。

   轮询后，SSL 证书和密钥文件将下载并添加到证书存储中。

   > 注意：
   >
   > 如果存储区中存在相同的证书名称，则证书的导入操作将失败。但是，导入操作会继续轮询剩余的证书，并将 NetScaler 证书（如果有）添加到存储中。

配置作业

January 29, 2024

NetScaler 控制台配置管理流程可确保在网络中的多个 NetScaler 实例上正确复制配置更改、系统升级和其他维护活动。

NetScaler 控制台允许您创建配置作业，帮助您在多台设备上作为一项任务轻松执行所有这些活动。配置作业和模板将最重复的管理任务简化为 NetScaler 控制台上的单个任务。配置作业包含可以在一个或多个托管设备上运行的一组配置命令。

配置作业可以使用 SSH 命令执行配置命令，也可以使用 SCP 将文件副本从本地存储复制到另一个设备，例如，可以计划 HA 故障转移或 HA 升级。

您可以在 NetScaler 控制台中使用以下四个选项之一来创建配置作业。使用其中一个创建可重复使用的命令和指令来源，用于系统运行配置作业。

1. 配置模板
2. 实例
3. 文件
4. 录制和播放

配置模板

您可以在创建作业并将一组配置命令另存为模板的同时创建配置模板。在“Create Jobs”（创建作业）页面上保存这些模板时，它们会自动显示在“Create Template”（创建模板）页面上。有关更多信息，请参见 如何在 NetScaler 控制台上使用主配置模板。

> 注意
>
> 默认配置模板的 重命名 选项处于禁用状态。但是，您可以重命名自定义配置模板。

您可以使用以下模板之一：

配置编辑器：您可以使用配置编辑器键入 CLI 命令，将配置保存为模板，然后使用它来配置作业。

内置模板：您可以从配置模板列表中进行选择。这些模板提供了 CLI 命令的语法，并允许您为变量指定值。下表中列出了内置模板及其说明。可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例如，可以使用内置模板选项计划作业来配置 syslog 服务器。您还可以选择立即运行作业或安排在稍后阶段运行作业。

有关更多信息，请参阅 如何使用配置模板创建审核模板

实例

您可以对运行 NetScaler 11.0 版及更高版本的 NetScaler SDX 实例执行单捆绑升级。要执行单包升级，可以在 NetScaler 控制台中使用内置任务。您还可以通过提取运行配置或保存的配置并在另一个同类型的 NetScaler 实例上运行命令来升级 NetScaler 实例。此升级允许您在另一个实例上复制一个实例的配置。

文件

您可以从本地计算机上载配置文件并创建作业。

使用文件的优势

- 您可以使用任何文本文件来创建可重用的配置命令源。
- 不需要进行任何种类的格式设置。
- 文件可以保存在您的本地计算机上。

您可以创建并保存新文件，也可以导入现有文件，然后运行命令。

录制和播放

使用创建作业，您可以输入自己的 CLI 命令，也可以使用录制和播放按钮从 NetScaler 会话中获取命令。运行作业时，将记录所选实例上的 ns.conf 中的更改并将其复制到 NetScaler 控制台。请参阅“如何使用录制和播放创建配置作业”。

导出此控制板的报告

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每日、每周或每月报告，并通过电子邮件或松弛消息发送报告。

> 注意
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

相关文章

- 如何在配置作业中使用 SCP (put) 命令
- 如何在配置作业中使用变量
- 如何使用更正命令创建配置作业

创建配置作业

January 29, 2024

作业是可以在一个或多个托管实例上创建并运行的一组配置命令。

您可以创建任务以跨实例更改配置。您可以使用 NetScaler 控制台 GUI 在网络 上的多个实例上复制配置，录制和播放配置任务，并将其转换为 CLI 命令。

您可以使用 NetScaler 控制台的配置任务功能来创建配置作业、发送电子邮件通知和检查所创建任务的执行日志。

要在 **NetScaler** 控制台上创建配置作业，请执行以下操作：

1. 导航到 基础结构 **>** 配置 **>** 配置任务。
2. 单击 创建作业。
3. 在“创建作业”页上的“选择配置”选项卡下，指定任务名称并从列表中选择 实例类型。
4. 在 配置源 列表中，选择要创建的配置作业模板。为选定模板添加命令。

    - 您可以输入命令或从保存的配置模板中导入现有命令。
    - 在配置作业中创建作业时，还可以在配置编辑器中添加不同类型的多个模板。
    - 从 配置源 列表中选择不同的模板，然后将模板拖到配置编辑器中。模板类型可以是 配置模板、内置模板、主配置、录制和播放、实例 和 文件。

    > 注意
    >
    > 如果您首次添加部署主配置作业模板，添加不同类型的模板，则整个作业模板将变为主配置类型。

    您还可以在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。您还可以在编辑配置作业时重新排列命令行并重新排序。

    您可以定义变量，使您能够为这些参数分配不同的值或跨多个实例运行作业。您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。单击“预览变量”选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。

    您可以为配置编辑器上的每个命令自定义回滚命令。要指定您的自定义命令，请启用自定义回滚选项。

    > 重要
    >
    > 事项要使自定义回滚生效，请完成“创建作业”向导。在“执行”选项卡中，从“命令失败”列表中选择“回滚成功命令”选项。

5. 在“选择实例”选项卡中，选择要运行配置审核的实例。

a) 在 NetScaler 高可用性对中，您可以在主节点或辅助节点的本地运行配置作业。选择要在哪个节点上运行作业。

- 在主节点上执行 -选择此选项可仅在主节点上运行作业。
- 在辅助节点上执行 -选择此选项可仅在辅助节点上运行作业。

您还可以选择主节点和辅助节点来运行同一配置作业。如果未选择主节点或辅助节点，配置作业将自动在主节点上运行。

b) 单击 添加实例，然后从列表中选择实例。单击确定。

c) 单击下一步。

6. 在“指定变量值”选项卡中，有两个选项：

a) 下载输入文件以输入您在命令中定义的变量的值，然后将该文件上载到 NetScaler 控制台服务器。

b) 输入您为所有实例定义的变量的通用值

c) 单击下一步。

7. 在“作业预览”选项卡上评估和验证要在每个实例上运行的命令。如果在“选择 配置”选项卡上指定，此选 项卡还会显示回滚命令。

8. 在“执 行”选项卡中，选择立即运行作业，或者安排稍后运行作业。

此外，从“命令失败”列表中选择以下操作之一，如果 命令失败，NetScaler 控制台必须执行该操作：

- 忽略错误并继续：NetScaler 控制台忽略失败的命令并为所选实例运行其余命令。

> 注意
>
> 此操作不允许您中止正在进行的配置作业。

- 停止进一步执行：如果任何命令在执行期间失败，NetScaler 控制台将停止其余命令。
- 回滚成功的命令：如果任何命令在执行期间失败，NetScaler 控制台将恢复成功运行的命令。

  如果启用了定制回滚，则 NetScaler 控制台会为失败的命令运行相应的回滚命令。

9. 单击完成。

要发送任务的电子邮件和 **Slack** 通知，请执行以下操作：

现在，每次运行或计划作业时，都会发送电子邮件和 Slack 通知。通知包括作业成功或失败等详细信息以及相关详细信息。

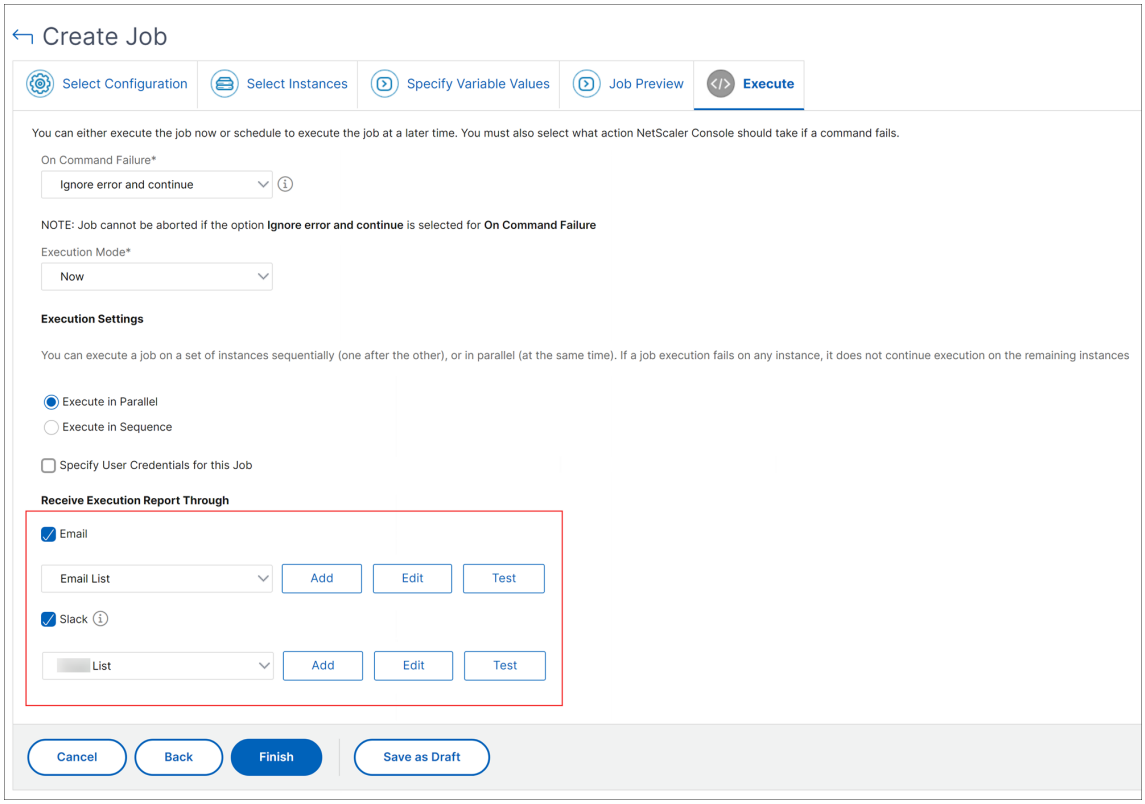
1. 导航到 基础结构 **>** 配置 **>** 配置作业。
2. 选择要启用电子邮件和 Slack 通知的作业，然后单击 编辑。
3. 在“执行”选项卡中，转到“通过以下方式接收执行报告”窗格：

- 选中“电子邮件”复选框，然后选择要向其发送执行报告的电子邮件分发列表。

  如果要添加电子邮件通讯组列表，请单击“添加”并指定电子邮件服务器的详细信息。

- 选中 **Slac** k 复选框，然后选择要向其发送执行报告的 Slack 频道。

  如果要添加 Slack 配置文件，请单击 添加 并指定所需 Slack 频道的配置文件名称、频道名称和 令牌。

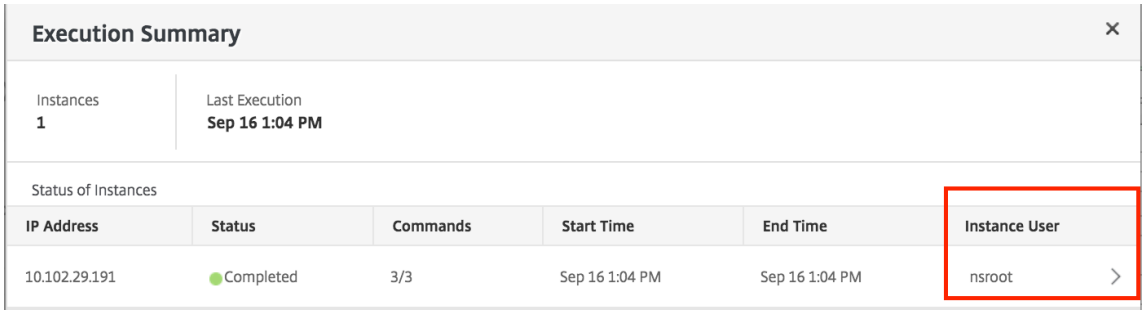


4. 单击完成。

要查看执行摘要详细信息，请执行以下操作：

1. 导航到 基础结构 **>** 配置 **>** 配置作业。
2. 选择要查看执行摘要的作业，然后单击 详细信息。
3. 单击“执行摘要”以查看：

   - 运行的作业上实例的状态
   - 这些命令在作业上运行
   - 作业的开始和结束时间，以及
   - 实例用户的名称



配置审核

January 29, 2024

本文档包括：

- 创建审核模板
- 查看审核报告
- 跨实例审核配置更改
- 获取有关网络配置的配置建议
- 如何轮询 NetScaler 控制台实例的配置审核
- 为 ConfigChange SNMP 陷阱生成配置审核差异

升级作业

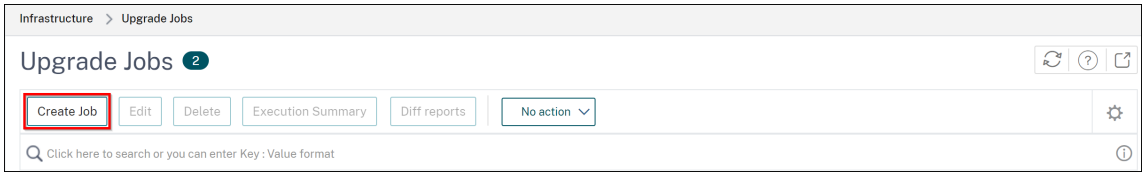
January 29, 2024

您可以使用 NetScaler 控制台创建以下维护任务。然后，您可以将维护任务安排在特定的日期和时间。

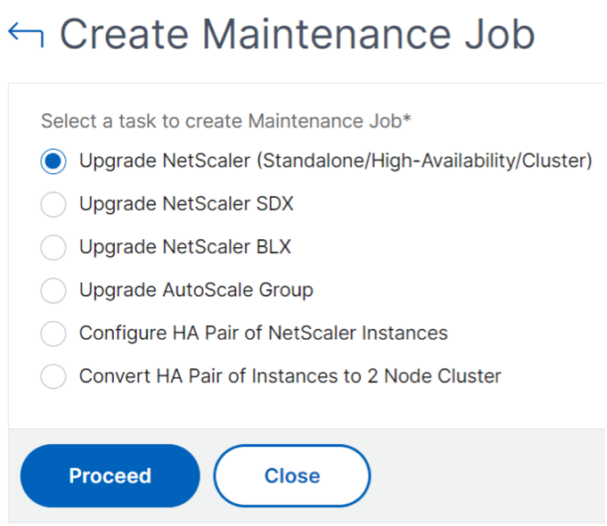
- 升级 NetScaler 实例
- 升级 NetScaler SDX 实例
- 升级 NetScaler BLX 实例
- 升级 AutoScale 组中的 NetScaler 实例
- 配置 NetScaler 实例的高可用性对
- 将 HA 实例对转换为群集

计划升级 **NetScaler** 实例

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 升级任务。单击 创建作业。



2. 在 创建维护作业中，选择 升级 **NetScaler**（独立/高可用性/群集），然后单击 继续。



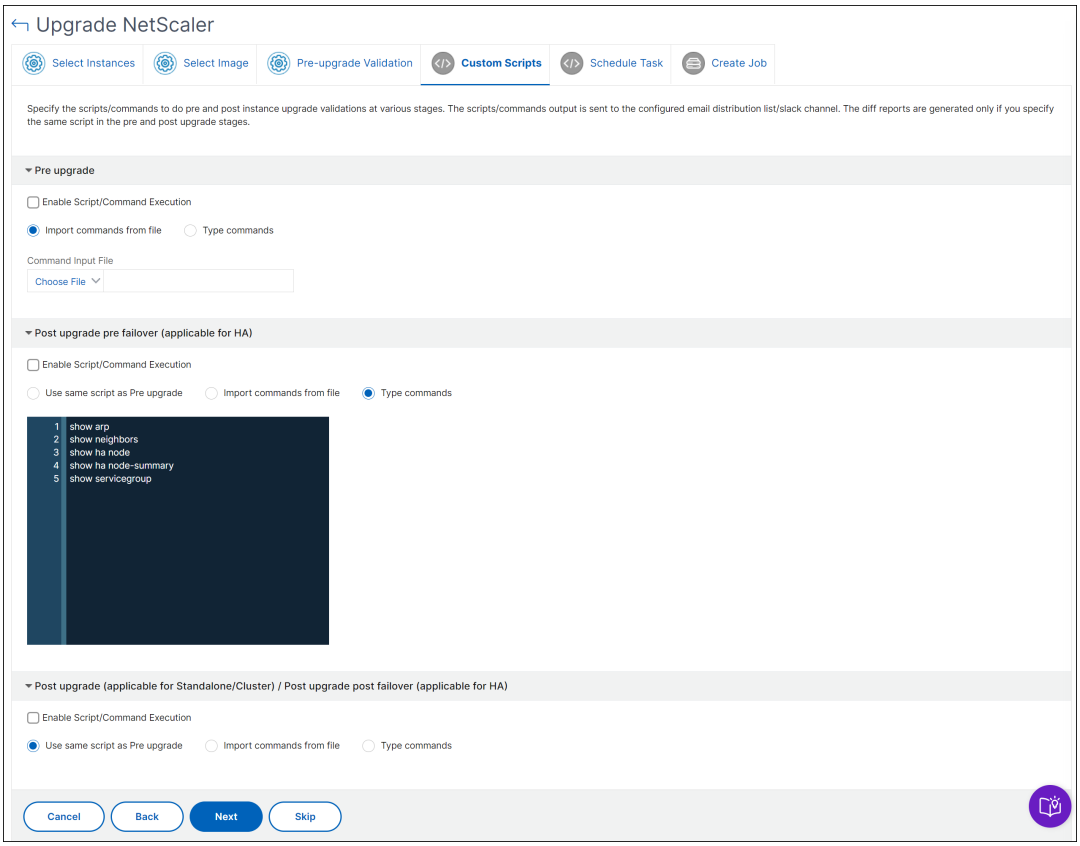
3. 在选择实例中，为作业名称键入您选择的名称。
4. 单击“添加实例”以添加要升级的 NetScaler 实例。
   - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。但是，建议使用主实例升级 HA 对。
   - 要升级群集，请指定群集 IP 地址。
5. 单击“下一步”选择映像。从“软件映像”列表中选择以下选项之一：
   - 本地 - 从本地计算机中选择实例升级文件。
   - 设备-从 NetScaler 控制台文件浏览器中选择实例升级文件。NetScaler 控制台 GUI 显示 `/var/mps/mps_images` 处存在的实例文件。
     - 如果 **@@** 所选图像已经可用，则跳过将图像上载到 NetScaler 的操作-如果该图像已存在于 NetScaler 实例中，则选择此选项。
     - 成功升级后从 **NetScaler** 清理软件映像 - 选择此选项可在实例升级后清除 NetScaler 实例中上载的映像。
6. 单击 下一步 开始对所选实例进行升级前验证。

   升级前验证选项卡显示失败的实例。删除失败的实例，然后单击下一步。

> 重要
>
> 如果您指定群集 IP 地址，则 NetScaler 控制台仅在指定的实例上进行升级前验证，不在其他群集节点上进行升级前验证。

7. 可选，在 自定义脚本中，指定要在实例升级之前和之后运行的脚本。使用以下方法之一来运行命令：

   - 从文件导入命令 -从本地计算机中选择命令输入文件。
   - 键入命令 - 直接在 GUI 上输入命令。



   可以使用自定义脚本在实例升级前后检查更改。例如：

   - 升级前后的实例版本。
   - 升级前后接口、高可用性节点、虚拟服务器和服务的状态。
   - 虚拟服务器和服务的统计信息。
   - 动态路由。

8. 单击下一步。在 计划任务中，选择以下选项之一：

   - 立即升级 -升级作业将立即运行。

- 稍后计划 -选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。

  如果要分两个阶段升级 NetScaler HA 对，请选择 **HA** 中的节点执行两阶段升级。

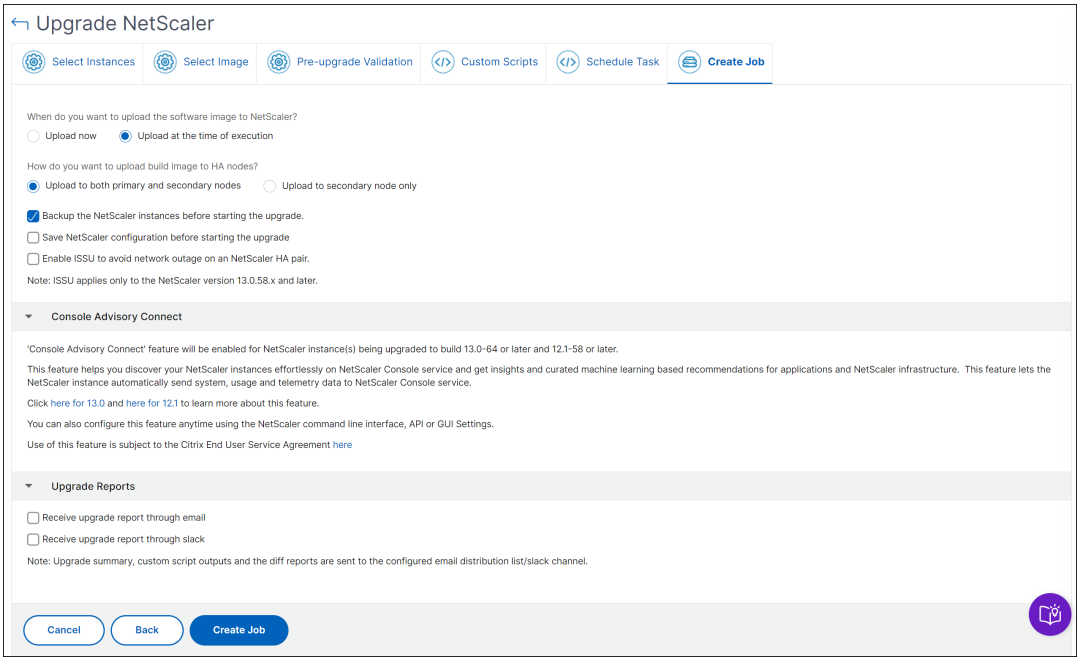
  如果要升级高可用性对中的其他实例，请指定执行日期和开始时间。

9. 单击下一步。在 创建作业中，指定以下详细信息：

   a) 指定您希望何时将映像上载到实例：

   - 立即上载 -选择此选项可立即上载图片。但是，升级作业将在计划的时间运行。
   - 执行时上载 -选择此选项可在升级作业执行时上载映像。
   - 在开始升级之前，请备份 **NetScaler** 实例。- 创建所选 NetScaler 实例的备份。
   - 开始升级之前保存 **NetScaler** 配置 -保存升级前在实例上配置的配置作业。
   - 启用 **ISSU** 以避免 **NetScaler HA** 对的网络中断 - ISSU 可确保 NetScaler 高可用性对的零停机升级。此选项提供了在升级期间支持现有连接的迁移功能。因此，您可以在不停机的情况下升级 NetScaler HA 对。以分钟为单位指定 ISSU 迁移超时。

   - 控制台公告连接-如果您要升级到 **13.0-64** 或更高版本以及 **12.1-58** 或更高 版本，控制台公告连接将自动启用。有关更多信息，请参阅 使用 NetScaler 控制台服务连接以低接触方式加载 NetScaler 实例。
   - 通过电子邮件接收执行报告 -通过电子邮件发送执行报告。要添加电子邮件通讯组列表，请参阅 创建电子邮件通讯组列表。
   - 通过松弛接收执行报告 -以松弛方式发送执行报告。要添加 Slack 配置文件，请参阅 创建 Slack 配置文件。



10. 单击 创建作业。

计划升级 **NetScaler SDX** 实例

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 升级任务。单击 创建作业。
2. 选择 升级 **NetScaler SDX** ，然后单击 继续。
3. 在 升级 **NetScaler SDX** 页面的 实例选择”选 项卡中：
   a) 添加任务名称。
   b) 从“软件映像”列表中，选择“****** 本 地”（您的本地计算机）或“** 设备”（编译文件必须存在于 NetScaler 控制台虚拟设备上）。

      上载过程开始。
   c) 添加要在其上运行升级过程的 NetScaler SDX 实例。
   d) 单击下一步。
4. 在“计划任务”选项卡上，从“执行模式”列表中选择“立即 升级 NetScaler SDX 实例”，然后单击完成。
5. 要稍后升级 NetScaler SDX 实例，请从 执行模式 列表中选择以 后。然后，您可以选择升级 NetScaler 实例的执行日期和开始时间，然后单击 完成
6. 您还可以启用电子邮件和 slack 通知以接收升级 NetScaler SDX 实例的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

   有关配置电子邮件通讯组列表和 Slack 通道的详细信息，请参阅 NetScaler 实例的计划升级中的步骤 **8**

计划升级 **NetScaler BLX** 实例

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 升级任务。单击 创建作业。
2. 在 创建维护作业中，选择 升级 **NetScaler BLX** ，然后单击 继续。
3. 在选择实例中，为作业名称键入您选择的名称。
4. 单击 添加实例 以添加要升级的 BLX 实例。
   - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。但是，建议使用主实例升级 HA 对。
   - 要升级群集，请指定群集 IP 地址。
5. 单击“下一步”以选择图像。从“软件映像”列表中选择以下选项之一：
   - 本地 - 从本地计算机中选择实例升级文件。
   - 设备-从 NetScaler 控制台文件浏览器中选择实例升级文件。NetScaler 控制台 GUI 显示 `/var/mps/mps_images` 处存在的实例文件。
     - 如果 **@@** 所选图像已经可用，则跳过将图像上载到 NetScaler 的操作-如果该图像已存在于 NetScaler 实例中，则选择此选项。

- 成功升级后从 **NetScaler** 清理软件映像 - 选择此选项可在实例升级后清除 NetScaler 实例中上载的映像。

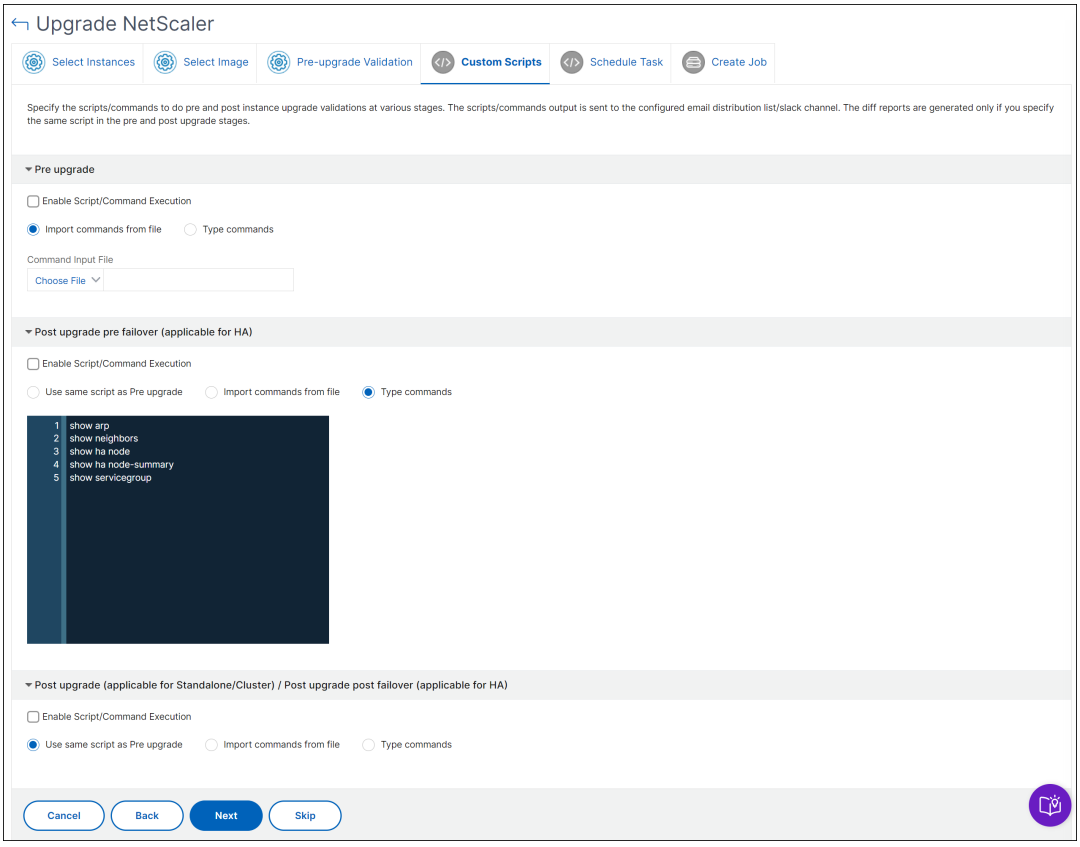
6. 单击 下一步 开始对所选实例进行升级前验证。

   升级前验证选项卡显示失败的实例。删除失败的实例，然后单击下一步。

   > 重要
   >
   > 如果您指定群集 IP 地址，则 NetScaler 控制台仅在指定的实例上进行升级前验证，不在其他群集节点上进行升级前验证。

7. 可选，在 自定义脚本中，指定要在实例升级之前和之后运行的脚本。使用以下方法之一来运行命令：

   - 从文件导入命令 -从本地计算机中选择命令输入文件。
   - 键入命令 - 直接在 GUI 上输入命令。



   可以使用自定义脚本在实例升级前后检查更改。例如：

   - 升级前后的实例版本。
   - 升级前后接口、高可用性节点、虚拟服务器和服务的状态。
   - 虚拟服务器和服务的统计信息。
   - 动态路由。

8. 单击下一步。在 计划任务中，选择以下选项之一：

   - 立即升级 -升级作业将立即运行。
   - 稍后计划 -选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。

     如果要分两个阶段升级 HA 对，请选择对高 可用性中的节点执行两阶段升级。

     如果要升级高可用性对中的其他实例，请指定执行日期和开始时间。

9. 单击下一步。在 创建作业中，指定以下详细信息：

   a) 指定您希望何时将映像上载到实例：

      - 立即上载 -选择此选项可立即上载图片。但是，升级作业将在计划的时间运行。
      - 执行时上载 -选择此选项可在升级作业执行时上载映像。
      - 在开始升级之前备份 **NetScaler** 实例 -创建所选 NetScaler 实例的备份。
      - 在开始升级之前保存 **NetScaler** 配置 -保存升级前在实例上配置的配置作业。
      - 启用 **ISSU** 以避免 **NetScaler HA** 对出现网络中断——ISSU 可确保 NetScaler 高可用性对的零停机升级。此选项提供了在升级期间支持现有连接的迁移功能。因此，您可以在不停机的情况下升级 NetScaler HA 对。以分钟为单位指定 ISSU 迁移超时。

   - 控制台公告连接-如果您要升级到 **13.0-64** 或更高版本以及 **12.1-58** 或更高 版本，控制台公告连接将自动启用。有关更多信息，请参阅使用控制台公告连接以 低接触方式加载 NetScaler 实例。
   - 通过电子邮件接收执行报告 -通过电子邮件发送执行报告。要添加电子邮件通讯组列表，请参阅 创建电子邮件通讯组列表。
   - 通过松弛接收执行报告 -以松弛方式发送执行报告。要添加 Slack 配置文件，请参阅 创建 Slack 配置文件。

10. 单击 创建作业。

计划升级自动扩展组

执行以下步骤以升级属于 AutoScale 组的云服务中的所有实例：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 升级任务。单击 创建作业。
2. 选择升级 **AutoScale** 组，然后单击继续。
3. 在 升级设置 选项卡中：

   a) 选择要升级的 **AutoScale** 组。

   b) 在映像中，选择 NetScaler 版本。此映像是 AutoScale 组中 NetScaler 实例的现有版本。

   c) 在 **NetScaler** 映像中，浏览要升级到的 NetScaler 版本文件。

      如果选中“平滑升级”，则升级任务将等到指定的耗尽连接期限到期。

d) 单击下一步。

4. 在“计划任务”选项卡中：

   a) 从“执行模式”列表中选择以下选项之一：

      - 现在：要启动 NetScaler 实例，请立即升级。
      - 稍后：稍后启动 NetScaler 实例升级。

   b) 如果选择“以 后 选项，请在要启动升级任务时选择“执行日期”和“开始时间”。

   您还可以启用电子邮件和松弛通知以接收升级 AutoScale 组的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

5. 单击完成。

安排配置 **NetScaler** 实例的高可用性对

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 升级任务。单击 创建作业。
2. 选择 配置 **NetScaler** 实例的 **HA** 对，然后单击 继续。
3. 在 **NetScaler HA** 对 页面的 实例选择”选 项卡中：

   a) 添加任务名称。

   b) 输入主 IP 地址。

   c) 输入辅助 IP 地址。

   d) 单击下一步。

   e) 如果您在两个子 网中有 **HA** 对实例，请单击以启用打开 **INC**（独立网络配置）模式。

4. 在计划任务选项卡上，从执行模式列表中选择立即立即升级 NetScaler 实例，然后单击完成。
5. 要稍后升级 NetScaler HA 对，请从 执行模式 列表中选择以 后。然后，您可以选择升级 NetScaler 实例的执行日期和开始时间，然后单击 完成。
6. 您还可以启用电子邮件和 slack 通知，以接收创建 NetScaler HA 对的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

   有关配置电子邮件分发列表和 Slack 频道的更多信息，请参见 Net Scaler 实例计划升级中的步骤 **8**。

计划将 **HA** 实例对转换为群集

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 升级任务。单击 创建作业。
2. 选择 将 **HA** 实例对转换为 **2** 节点群集，然后单击 继续。

3. 在 将 **NetScaler HA** 迁移到群集 页上的 实例选择”选 项卡中，添加 任务名称。指定主 IP 地址、辅助 IP 地址、主节点 ID、辅助节点 ID、群集 IP 地址、群集 ID 和背板，然后单击 下一步。
4. 在计划任务选项卡上，从执行模式列表中选择立即立即升级 NetScaler 实例，然后单击完成。
5. 要稍后升级，请从“执行模式”列表中选择以 后。然后，您可以选择升级 NetScaler HA 对实例的 执行日期 和开始时间，然后单击 完成。
6. 您还可以启用电子邮件和 slack 通知以接收升级 NetScaler SDX 实例的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

   有关配置电子邮件分发列表和 Slack 频道的更多信息，请参见 Net Scaler 实例计划升级中的步骤 **8**。

使用作业升级 **NetScaler** 实例

September 2, 2024

在 NetScaler 控制台中，您可以升级一个或多个 NetScaler 实例。在升级实例之前，您必须了解许可证框架和许可证类型。

注意：如果您想升级具有经典策略的实例，我们建议您在升级实例之前使用 NSPEPI 工具将经典策略转换为高级策略。这适用于 NSPEPI 工具支持的功能。有关更多信息，请参阅使用经典策略的配置的升级注意事项。

必备条件

NetScaler 控制台对要升级的实例执行以下预验证检查：

1. 检查磁盘空间 -清理磁盘空间以获得足够的磁盘容量进行实例升级。解决磁盘问题（如果有）。
2. 检查磁盘硬件问题 -解决硬件问题（如果有）。
3. 检查自定义项 -备份您的自定义项并从实例中删除它们。实例升级后，您可以重新应用备份的自定义设置。
4. 策略问题 -NetScaler 不支持版本中13.1的经典策略。将实例升级到此版本之前，请将经典策略迁移到高级策略。

   有关更多信息，请参阅 经典和高级策略。

自定义 **NetScaler** 配置的升级注意事项

重要的是，升级更改和自定义设置都应用于升级后的 NetScaler 设备。因此，如果您在 /etc 目录中有自定义配置文件，请在继续升级 NetScaler 设备之前，参阅自定义配置文件的升级注意事项。以下是您必须执行的主要步骤：

1. NetScaler 中的预升级步骤

- 升级前备份自定义文件
- 升级前删除自定义文件的符号链接

2. 使用 ADM 升级 NetScaler。要升级，请按照页面开头提供的说明进行操作。
3. NetScaler 中的升级后步骤

   - 升级后恢复自定义

升级前和升级后步骤都要在每个 NetScaler 实例上执行。但是，在步骤 2 中，要使用 ADM 升级 NetScaler，可以选择所有易受攻击的 NetScaler 实例并一起升级。

NetScaler 高可用性对

升级 NetScaler 高可用性对时，请注意以下几点：

- 首先升级辅助节点。
- 在两个节点成功升级之前，禁用节点的同步和传播。
- 成功升级高可用性对后，执行历史记录中将显示一条错误消息。如果高可用性对中的节点位于不同的版本或版本上，则会显示此消息。它表示主节点和辅助节点之间的同步已禁用。

您可以分两个阶段升级 NetScaler 高可用性对：

1. 创建升级作业并立即在其中一个节点上运行，或稍后安排。
2. 安排稍后在其余节点上运行升级作业。确保在初始节点升级后安排此作业。

NetScaler 群集

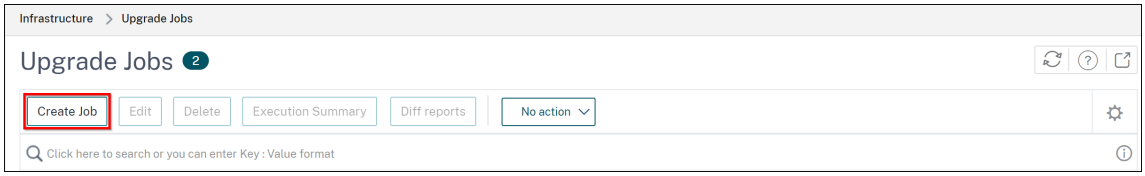
升级 NetScaler 群集时，在升级前的验证阶段，NetScaler 控制台仅验证指定的实例。因此，请检查并解决群集节点上的以下问题：

- 自定义
- 磁盘使用情况
- 硬件问题

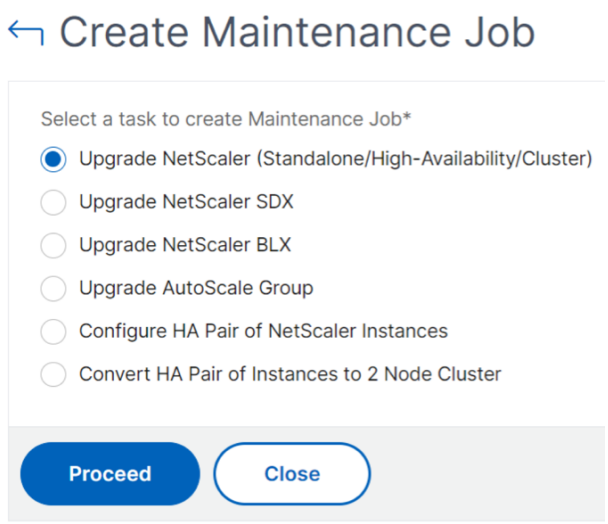
创建 NetScaler 升级任务

要创建 NetScaler 升级任务，请执行以下操作：

1. 导航到基础结构 **>** 升级作业。



2. 在 创建维护作业中，选择 升级 **NetScaler**（独立/高可用性/群集），然后单击 继续。



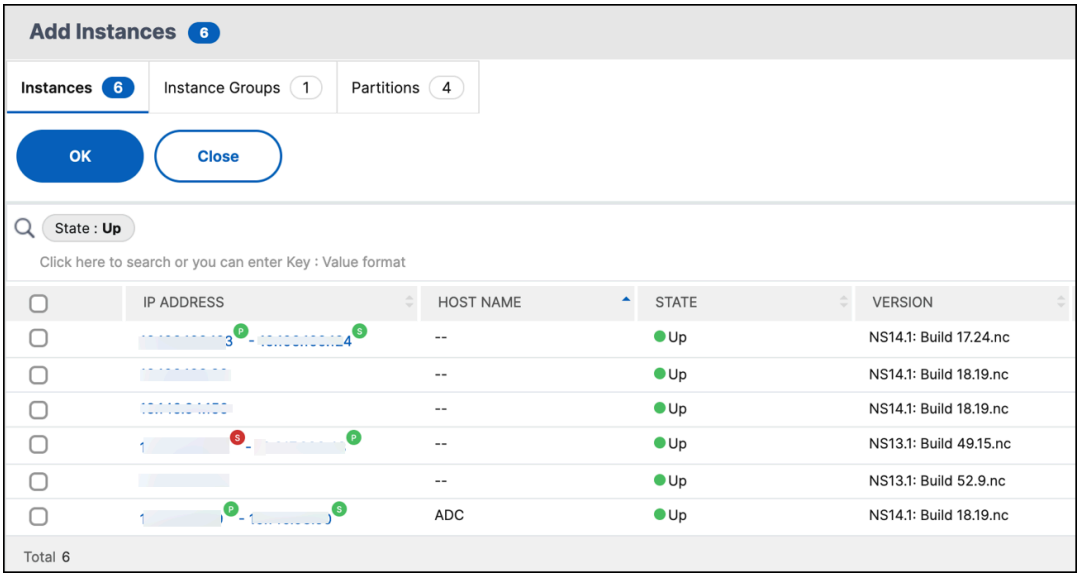
> 注意：
>
> 要升级 Autoscale 组，请参阅 升级自动缩放组。

3. 在“选择实例”选项卡中，

   a) 为 作业名称指定您选择的名称。

   b) 单击“添加实例”以添加要升级的 NetScaler 实例。

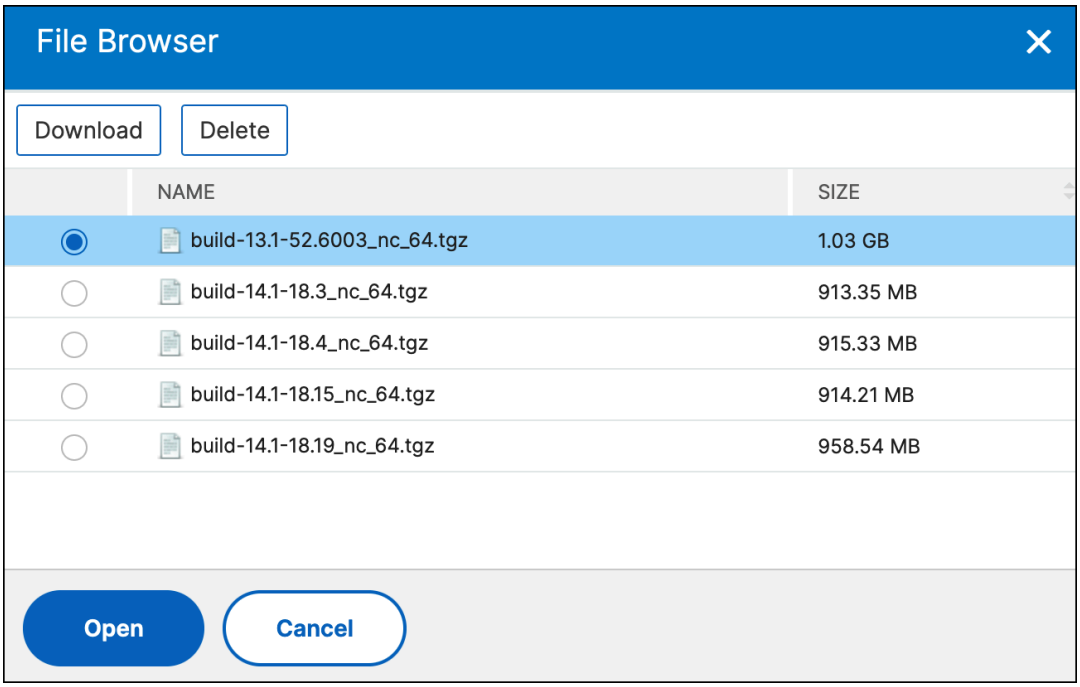
      - 要升级 NetScaler 高可用性对，请选择高可用性对的 IP 地址（用“S”和“P”的上标表示）。
      - 要升级群集，请选择群集 IP 地址（由“C”的上标表示）。



c) 单击确定。

4. 在“选择映像”标签中，从映像库或本地或设备中选择 NetScaler 镜像。

- 从映像库中选择：从列表中选择 NetScaler 镜像。此选项列出了 NetScaler 下载网站上提供的所有 NetScaler 镜像。



NetScaler 软件映像显示带有星形图标的首选版本。此外，大多数下载的版本都带有书签图标。

- 从本地或设备中选择：您可以从本地电脑或 NetScaler 设备上载图像。当您选择 NetScaler 设备时，NetScaler 控制台 GUI 会显示 `/var/mps/ns_images` 中存在的实例文件。从 NetScaler 控制台 GUI 中选择镜像。

- 如果所选图像已经可用，则跳过将图像上载到 **NetScaler** -此选项检查所选图像在 NetScaler 中是否可用。升级任务会跳过上载新映像，而使用 NetScaler 中可用的映像。
- 成功升级后从 **NetScaler** 清理软件映像 - 此选项将在实例升级后清除 NetScaler 实例中上载的映像。

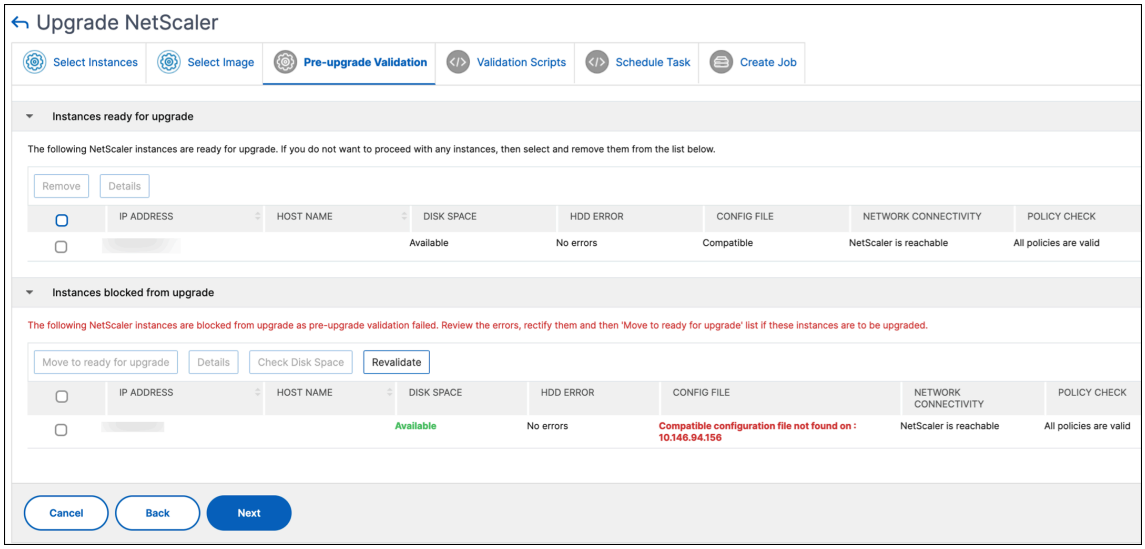
单击 下一步 开始对所选实例进行升级前验证。

> 注意：
>
> - 下载的 NetScaler 映像存储在代理中并存在于 `/var/mps/adcimages` 中。这些缓存的映像可用于多次 NetScaler 升级，因此无需每次升级都下载映像。
> - NetScaler 控制台根据镜像的最后修改时间每三天清除缓存的 NetScaler 镜像。一次只能在代理中缓存最新的两个图像文件。

5. 升级前验证选项卡显示以下部分：

   - 实例已准备好升级。您可以继续升级这些实例。
   - 实例无法升级。由于升级前的验证错误，这些 NetScaler 实例被禁止升级。

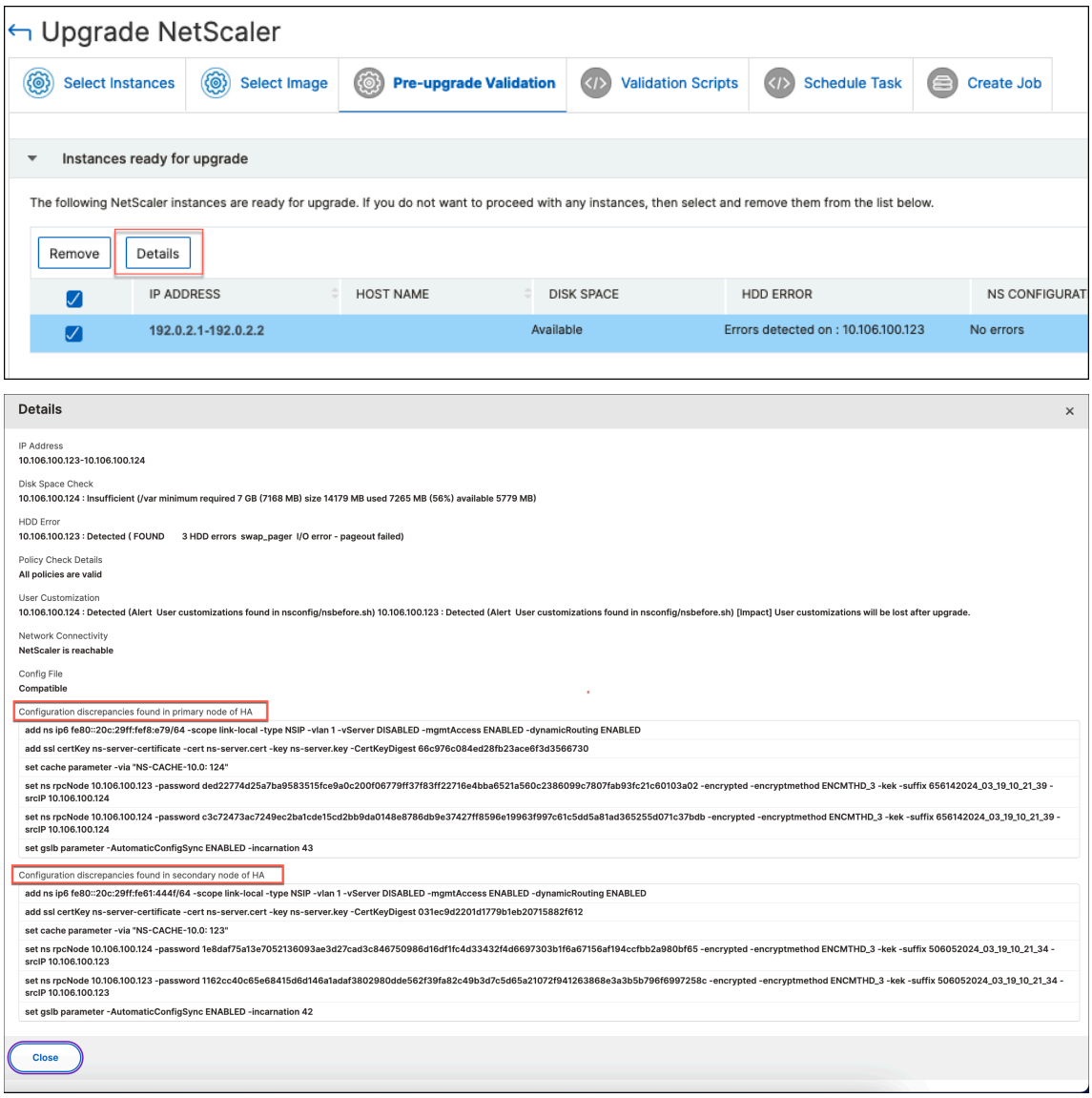
     您可以查看、更正错误，然后单击“移至准备升级”对其进行升级。如果实例上的磁盘空间不足，则可以检查并清理磁盘空间。请参阅清理 NetScaler 磁盘空间。



   - 策略检查：如果 NetScaler 控制台发现不支持的经典策略，您可以删除此类策略以创建升级任务。

> 重要：
>
> 如果您指定群集 IP 地址，则 NetScaler 控制台仅在指定的实例上进行升级前验证，不会在其他群集节点上进行升级前验证。

要查看升级期间主节点和辅助节点之间的差异，请选择高可用性节点，然后单击“详细信息”。



- 在高可用性的主节点中发现的配置差异 - 显示在 NetScaler 高可用性对的辅助节点中找到但在主节点中缺失的所有配置。
- 在高可用性的辅助节点中发现的配置差异 - 显示在 NetScaler 高可用性对的主节点中找到但在辅助节点中缺失的所有配置。

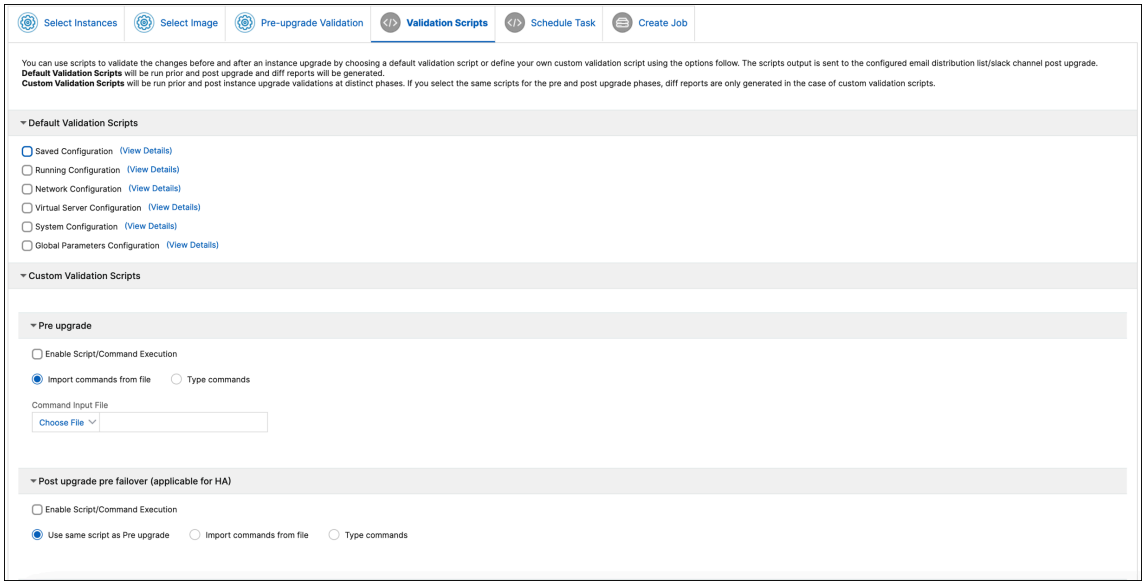
> 注意：
>
> 您可以忽略配置差异部分中可能出现的以下差异：
>
> - 特定设备的配置，如 IP 地址。
> - 加密的密码或证书，即使密码相同，节点之间也可能有所不同。
>
> 您可以查看差异，如果它们不相关，则选择忽略它们。

6. 在 验证脚本中，指定要在实例升级之前和之后运行的脚本。可以执行以下任一操作：

- 默认验证脚本 -选择此选项可运行预定义的验证脚本。这些脚本在升级任务之前和之后都运行，为验证脚本生成差异报告。

  > 注意：
  >
  > 您无法更改或编辑这些预定义的命令集。

- 自定义验证脚本 -选择此选项可运行您自己的验证脚本。您可以指定是否要在升级之前或之后运行脚本。只有在升级之前和之后选择了相同的脚本时，才会生成差异报告。



要了解每种配置中的命令集，请单击“查看详细信息”。

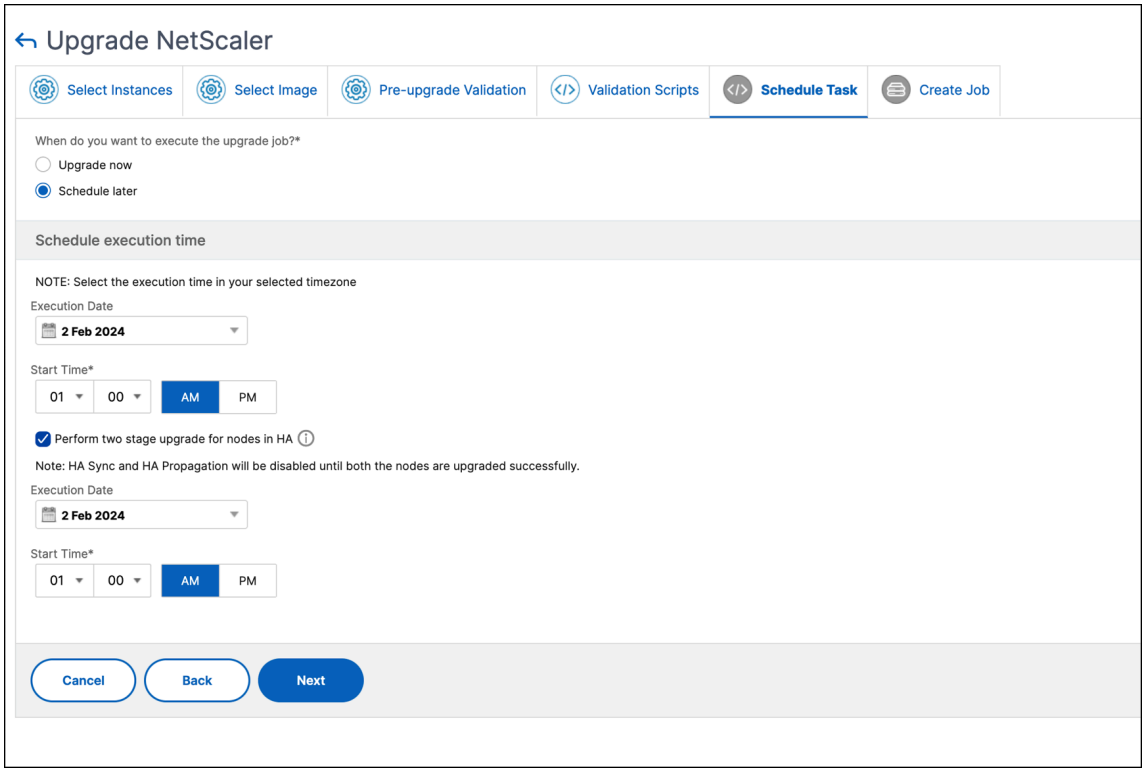
有关更多信息，请参阅 使用自定义脚本。

7. 在 计划任务中，选择以下选项之一：

   - 立即升级：升级作业将立即运行。
   - 稍后计划：选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。

   如果要分两个阶段升级 NetScaler 高可用性对，请选择对高可用性节点执行两阶段升级。

   如果要升级高可用性对中的另一个实例，请指定 执行日期 和 开始时间。



有关更多信息，请参见 NetScaler 高可用性对。

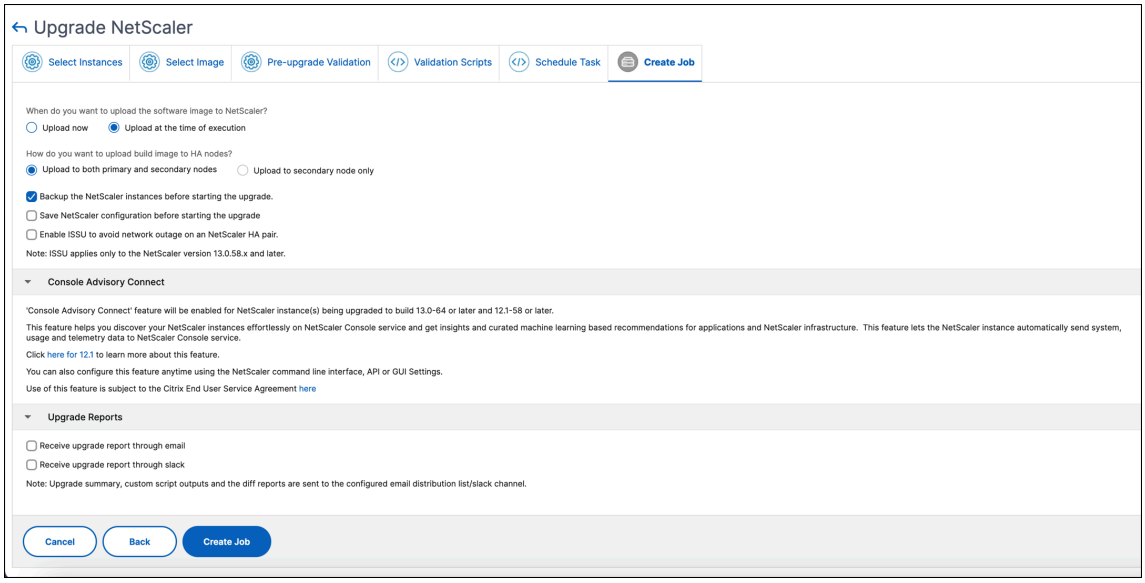
8. 在 创建作业中，指定以下详细信息：

   如果您安排升级作业，则可以指定要将映像上载到实例的时间：

   - 立即上载：选择此选项可立即上载图片。但是，升级任务将在预定时间运行。
   - 执行时上载：选择此选项可在升级任务执行时上载映像。

   对于高可用性对，您可以指定要上载图像的节点：

   - 上载到主节点和辅助节点：将构建映像文件上载到主节点和辅助节点。
   - 仅上载到辅助节点：仅将构建映像文件上载到辅助节点。升级辅助节点后，会发生故障转移，并将构建映像文件上载到新的辅助节点，该辅助节点以前是主节点。



有关高可用性对的可用计划方案的更多信息，请参见为 NetScaler 高可用性对计划升级作业。

有关其他升级选项的更多信息，请参见 NetScaler 升级选项。

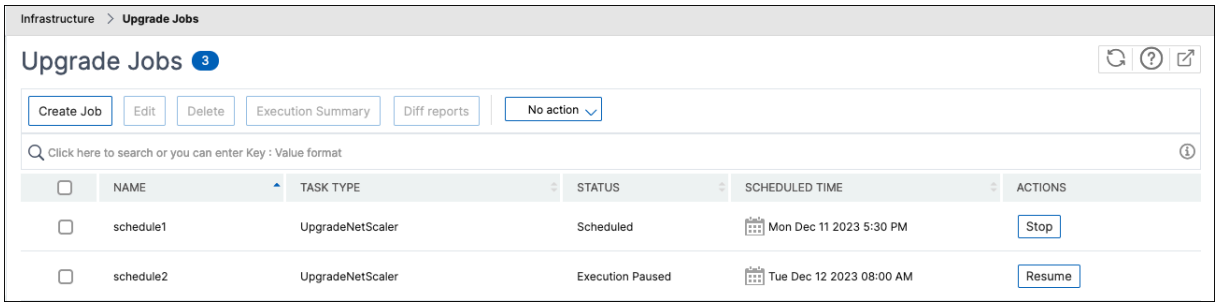
9. 单击 创建作业。

升级作业出现在 基础架构 **>** 升级作业中。编辑现有作业时，如果必填字段已填充，则可以切换到任何选项卡。例如，如果您位于“选择配置”选 项卡中，则可以切换到“作业预览”选项卡。

暂停或恢复预定的升级作业

您也可以暂停预定的升级任务。

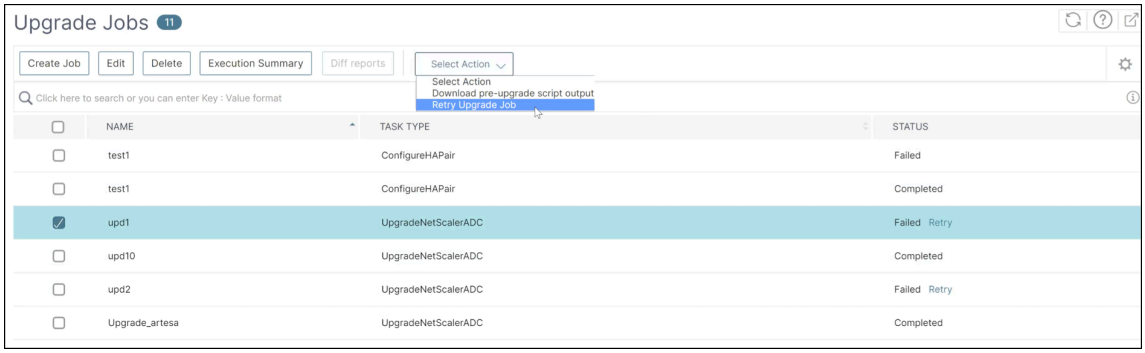
要使用此功能，请导航到 基础架构 **>** 升级作业，选择现有的计划升级作业，然后单击“停 止”以暂停作业。要恢复预定的升级作业，请单击“继续”。



> 注意：
>
> 如果在决定恢复升级任务后已过了计划时间，则需要重新创建升级作业。

重试失败的升级作业

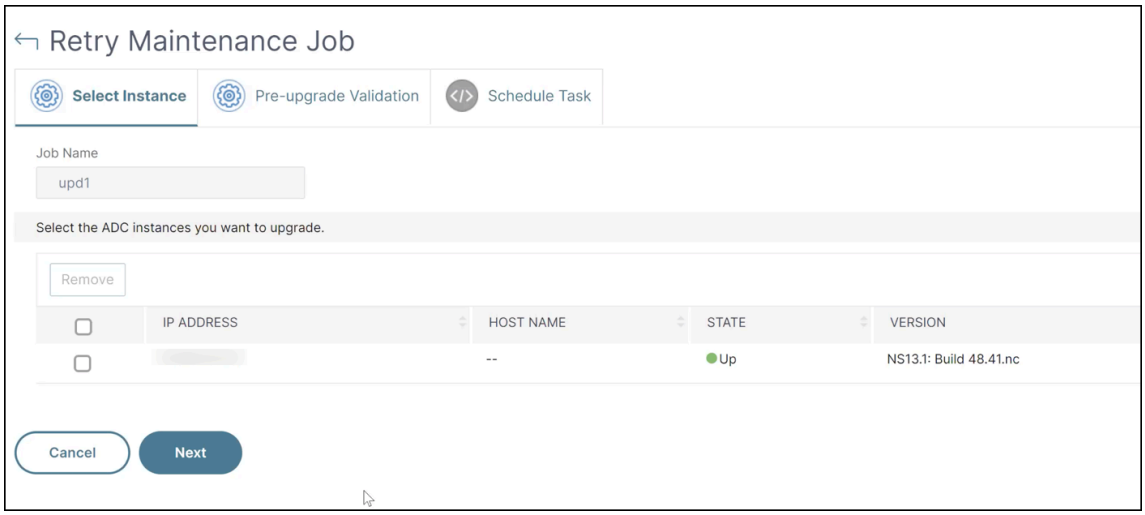
1. 在 基础架构 > 升级任务中，选择失败的升级任务，然后单击“重试”。或者，您也可以转到“选择操作” > “重试升级作业”以重试失败的作业。



2. 在 选择实例中，指定以下详细信息：

   - 任务名称 -输入升级的名称。
   - 从列表中选择要升级的 NetScaler 实例。要删除任何实例，请单击“移除”。

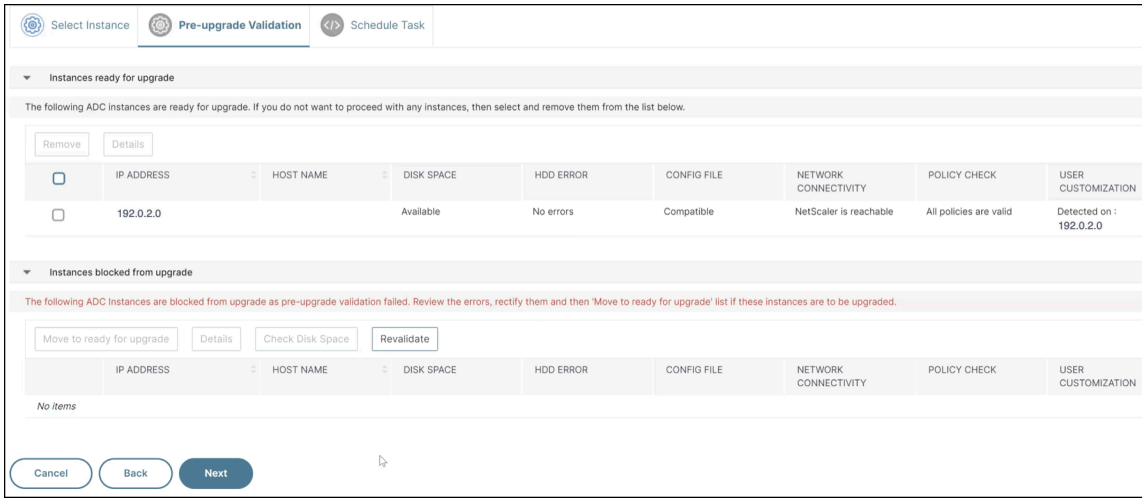
   单击“下一步”开始验证过程。



3. 升级前验证选项卡显示以下部分：

   - 实例已准备好升级。您可以继续升级这些实例。
   - 实例无法升级。由于升级前的验证错误，这些 NetScaler 实例被禁止升级。

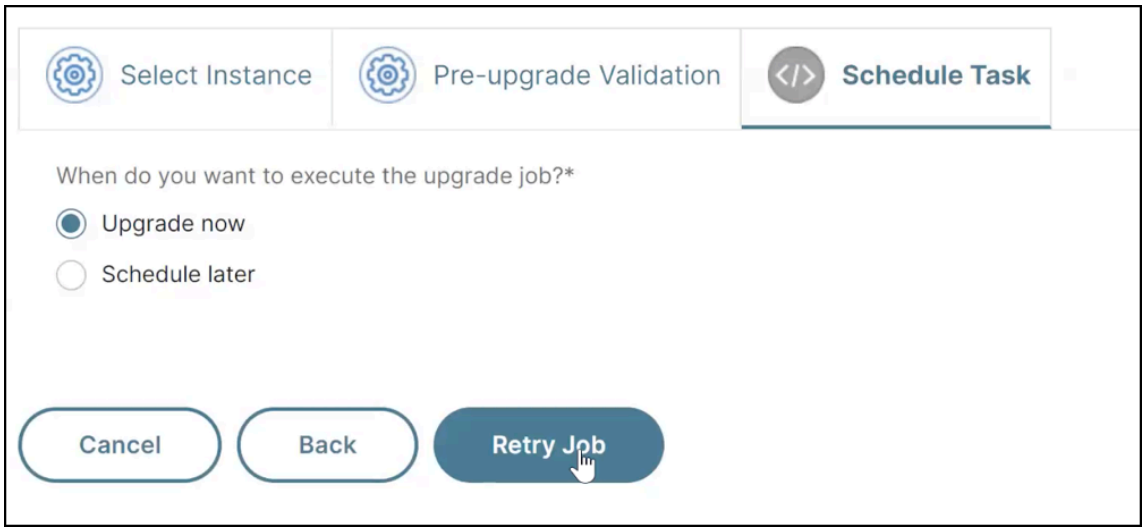
     您可以查看、更正错误，然后单击“移至准备升级”对其进行升级。如果实例上的磁盘空间不足，则可以检查并清理磁盘空间。请参阅清理 NetScaler 磁盘空间。
   - 策略检查：如果 NetScaler 控制台发现不支持的经典策略，您可以删除此类策略以创建升级任务。



单击下一步。

4. 在 计划任务中，选择以下选项之一：

   - 立即升级：升级作业将立即运行。
   - 稍后计划：选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。



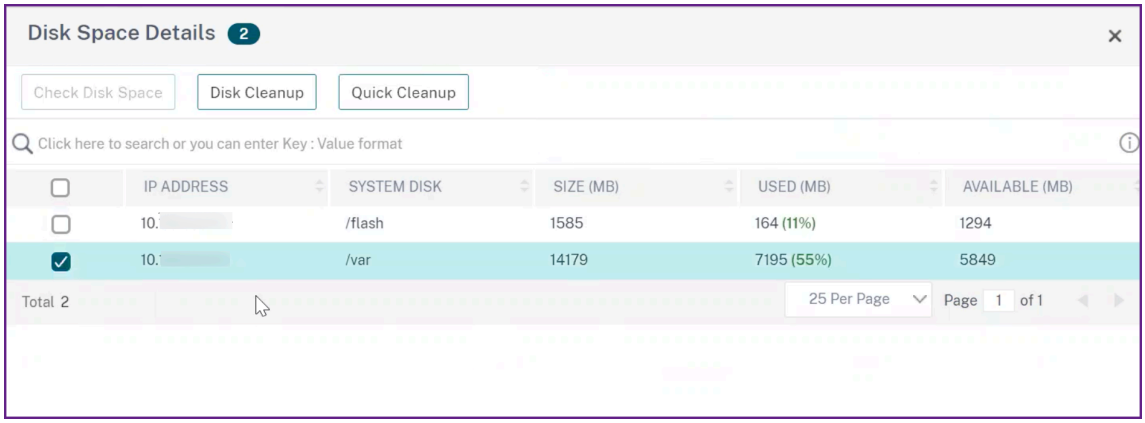
单击重试。

清理 **NetScaler** 的磁盘空间

如果您在升级 NetScaler 实例时遇到磁盘空间不足的问题，请从 NetScaler 控制台 GUI 本身清理磁盘空间。

1. 在升级前验证选项卡中，阻止升级的实例部分显示了由于磁盘空间不足而升级失败的实例。选择存在磁盘空间问题的实例。
2. 单击“检查磁盘空间”。

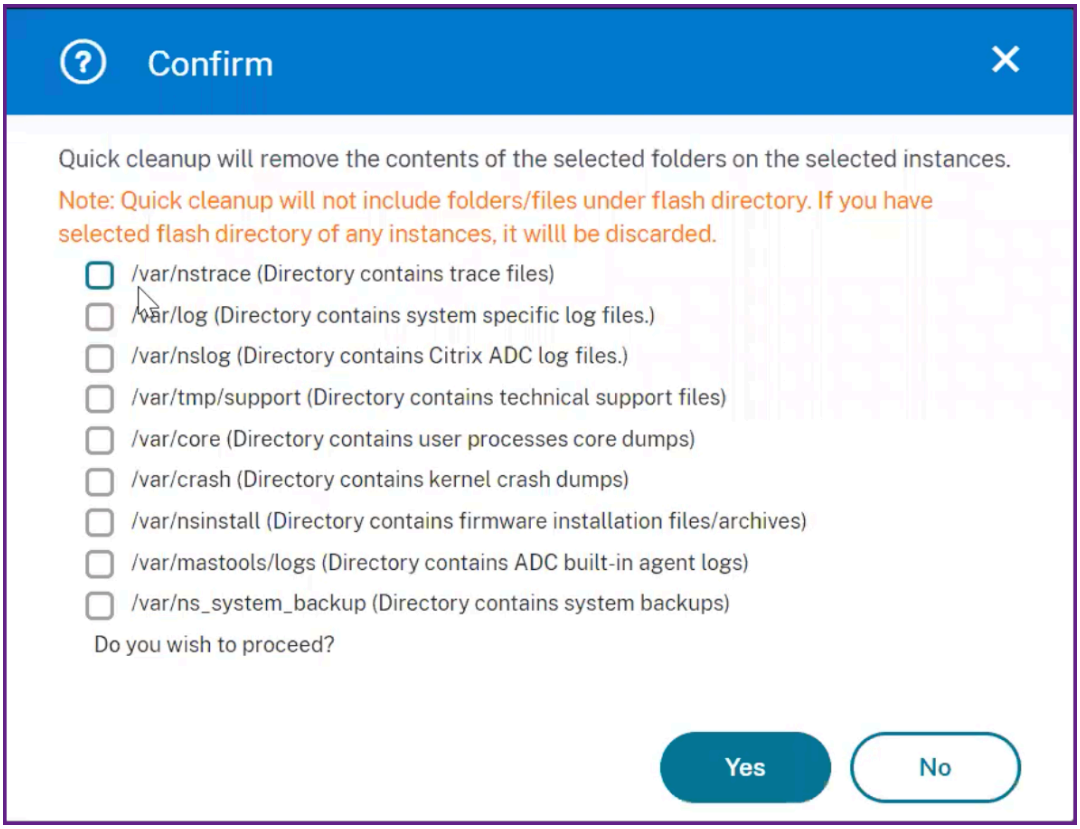
此时将出现“磁盘空间详细信息”窗格。此窗格显示实例、已用内存和可用内存。



3. 在“磁盘空间详细信息”窗格中，选择需要清理的实例，然后执行以下操作之一：

   a) 磁盘清理 - 导航到所需的文件夹或目录并将其删除以释放磁盘空间。

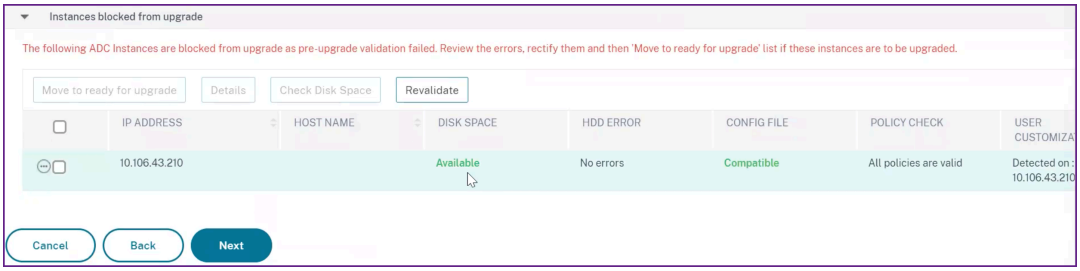
   b) 快速清理 - 通过删除多个文件夹来快速清理磁盘空间。在出现的“确认”窗格中，选择要删除的文件夹，然后单击“是”。



   c) 清理磁盘空间后，您可以检查现在是否有足够的磁盘空间可用于升级实例。在“阻止升级的实例”部分中，单击“重新验证”。

   在以下示例中，磁盘空间可用。现在，您可以单击“移至准备升级”来升级实例，或者单击“下一步”继续

执行下一步。



使用自定义脚本

在 创建 NetScaler 升级任务时，您可以指定定制脚本。定制脚本用于检查 NetScaler 实例升级之前和之后的更改。例如：

- 升级前后的实例版本。
- 升级前后接口、高可用性节点、虚拟服务器和服务的状态。
- 虚拟服务器和服务的统计信息。
- 动态路由。

指定要在以下阶段运行的自定义脚本：

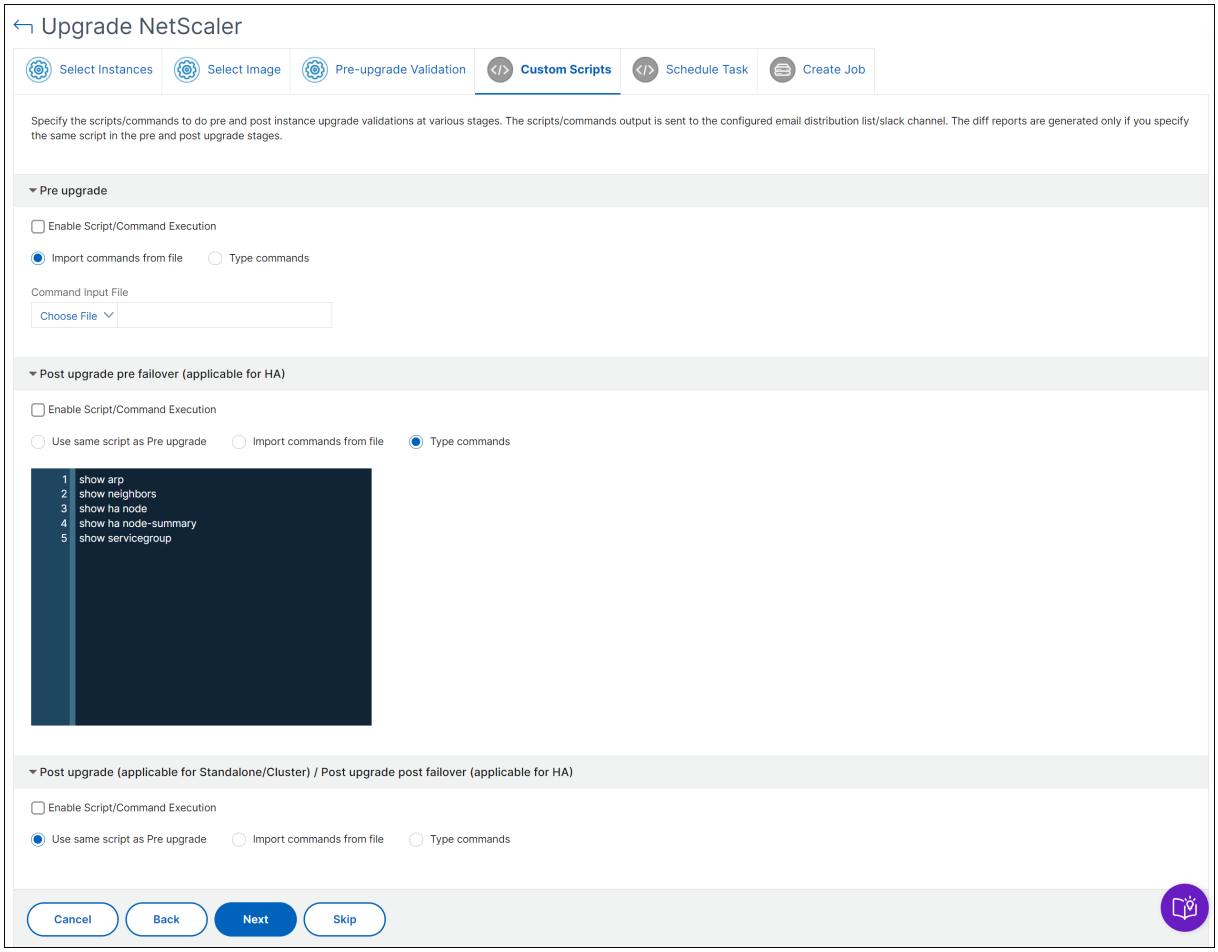
- 升级前：指定的脚本在升级实例之前运行。
- 升级后故障转移前（适用于 **HA**）：此阶段仅适用于高可用性部署。指定的脚本在升级节点之后但在其故障转移之前运行。
- 升级后（适用于独立版）**/**故障转移后升级后（适用于 **HA**）：指定的脚本在独立部署中升级实例后运行。在高可用性部署中，脚本在升级节点及其故障切换后运行。

> 注意：
>
> - 确保在所需阶段启用脚本或命令执行。否则，指定的脚本将不会运行。
> - 只有在升级前和升级后阶段指定了相同脚本时，才会生成差异报告。因此，请确保在升级后阶段选择“使用与升级前相同的脚本”。参见，下载 NetScaler 升级任务的合并差异报告。

您可以直接在 NetScaler 控制台 GUI 中导入脚本文件或键入命令。

- 从文件导入命令：从本地计算机中选择命令输入文件。
- 键入命令：直接在 GUI 上输入命令。

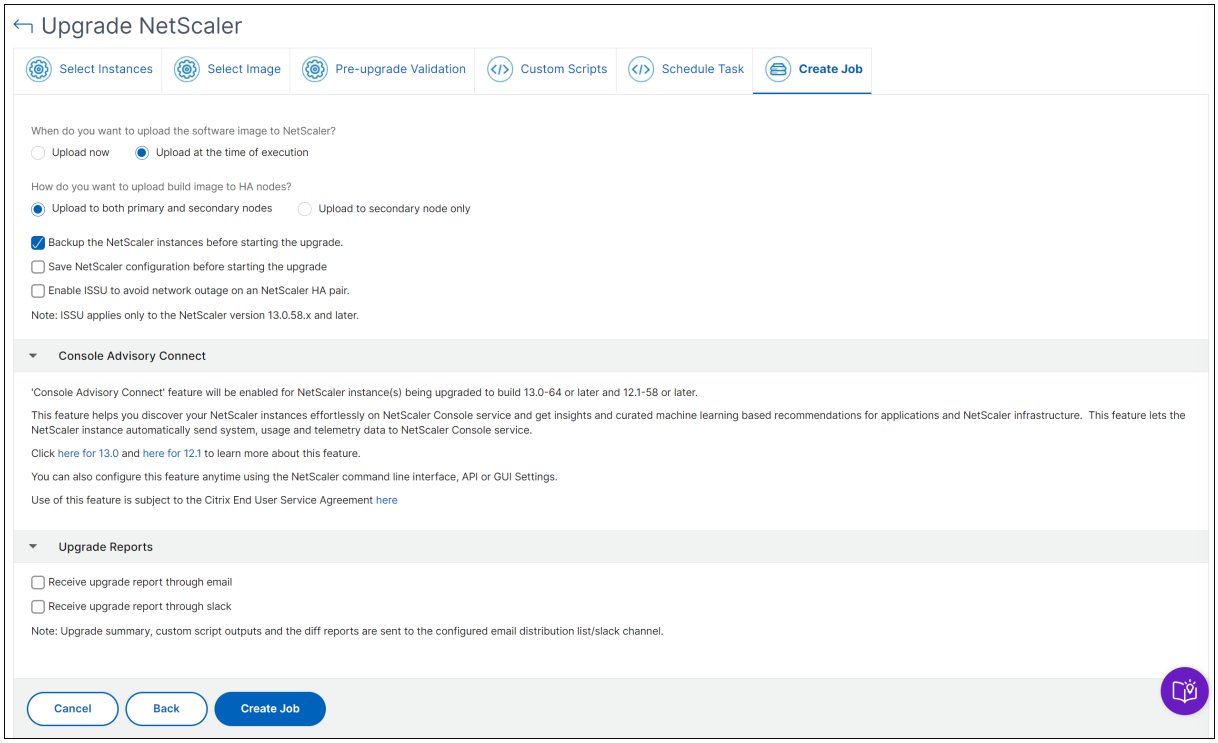
在升级后阶段，您可以使用在升级前阶段指定的相同脚本。



NetScaler 升级选项

创建 NetScaler 升级任务时，可以在“创建作业”选项卡中选择以下选项：

- 在开始升级之前，请备份 **NetScaler** 实例。：创建所选 NetScaler 实例的备份。
- 升级后保持高可用性节点的主要和辅助状态：如果您希望升级作业在每个节点升级后启动故障转移，请选择此选项。通过这种方式，升级作业将保持节点的主和次要状态。
- 在开始升级之前保存 **NetScaler** 配置 - 在升级 NetScaler 实例之前保存正在运行的 NetScaler 配置。
- 启用 **ISSU** 以避免 **NetScaler HA** 对出现网络中断——ISSU 可确保 NetScaler 高可用性对的零停机升级。此选项提供了在升级期间支持现有连接的迁移功能。因此，您可以在不停机的情况下升级 NetScaler 高可用性对。以分钟为单位指定 ISSU 迁移超时。
- 通过电子邮件接收执行报告 -通过电子邮件发送执行报告。要添加电子邮件通讯组列表，请参阅 创建电子邮件通讯组列表。
- 通过松弛接收执行报告 -以松弛方式发送执行报告。要添加 Slack 配置文件，请参阅 创建 Slack 配置文件。



为 **NetScaler** 高可用性对安排升级作业

下表列出了“调度 任务”页面中的不同调度方案，以及“创建作业”页面中可用的相应升级选项：

您想何时执行升级作业？	您想何时将软件映像上载到 **NetScaler**？	您想如何将构建映像上载到 **HA** 节点？
立即升级	不适用	上载到主节点和辅助节点（默认选项）
稍后安排	执行时上载（默认选项）	上载到主节点和辅助节点（默认选项）
稍后安排（选择在 **HA** 中对节点执行两阶段升级 时）	执行时上载（默认选项）	立即上载 仅上载到辅助节点（默认和唯一选项） 立即上载

下载 **NetScaler** 升级任务的合并差异报告

在 NetScaler 控制台中，您可以下载 NetScaler 升级任务的差异报告。为此，升级作业必须有 自定义脚本。差异报告包含升级前脚本和升级后脚本输出之间的差异。通过此报告，您可以确定 NetScaler 实例在升级后发生了哪些更改。

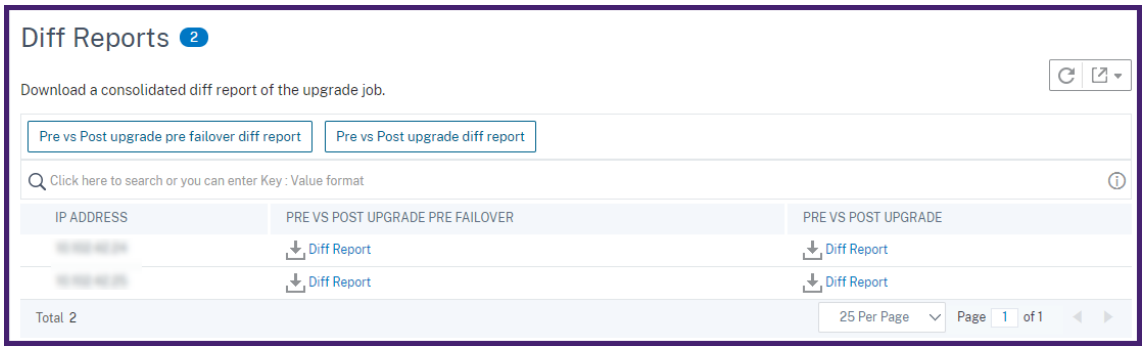
> 注意：
>
> 只有在升级前和升级后阶段指定相同的脚本时，才会生成差异报告。

要下载升级作业的差异报告，请执行以下操作：

1. 导航到 基础结构 > 配置作业 > 维护作业。
2. 选择要下载差异报告的升级作业。
3. 单击 差异报表。
4. 在 差异报告中，下载所选升级作业的合并差异报告。

   在此页面中，您可以下载以下任何差异报告类型：

   - 升级前与升级后的故障转移前差异报告
   - 升级前与升级后差异报告



网络功能

January 29, 2024

使用网络功能功能，您可以监视在托管的 Citrix 应用程序 Delivery Controller (NetScaler) 实例上配置的实体的状态。您可以查看统计信息，例如，事务详细信息、连接详细信息以及负载平衡虚拟服务器的吞吐量。您还可以在计划维护时启用或禁用实体。

“Network Functions”（网络功能）控制板为您提供以下图形：

- 客户端连接数最高的前 5 位虚拟服务器
- 服务器连接数最高的前 5 位虚拟服务器
- 吞吐量（MB/秒）最大的前 5 位虚拟服务器
- 吞吐量（MB/秒）最小的前 5 位虚拟服务器

- 虚拟服务器最多的前 5 位实例
- 虚拟服务器的状态
- 负载平衡虚拟服务器的运行状况
- 协议
- 负载平衡方法
- 负载平衡持久性

生成负载平衡实体的报告

January 29, 2024

NetScaler 控制台允许您查看所有级别的 Citrix Application Delivery Controller (NetScaler) 实例实体的报告。您可以在 **NetScaler** 控制台 **>** 网络 功能中下载两种类型的报告：合并报告和个人报告。

合并报告：您可以下载和查看在 NetScaler 实例上管理的所有实体的合并报告或汇总报告。

此报告允许您大致了解 NetScaler 实例、分区和网络中存在的相应负载平衡实体（虚拟服务器、服务组和服务）之间的映射。

下图显示了一个汇总报告示例。

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	AppDB		Load Balancing	test_ssl[redacted]		svc2[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1#[redacted]		svc1[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1#[redacted]		svc2[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS#[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1[redacted]	

合并报告的格式为 CSV 格式。每列中的条目说明如下：

- **NetScaler IP** 地址：NetScaler 实例的 IP 地址显示在报告中
- **NetScaler** 主机名：主机名显示在报告中。
- 分区：显示管理分区的 IP 地址
- 虚拟服务器:<name_of_the_virtual_server>#virtual_IP_address: port_number
- 服务：<name_of_the_service>#service-IP_address:port_number
- 服务组:<name_of_service_group>#server_member1_IP_address: Port、server_member2_IP_address: Port、server_member3_IP_address: Port、…，server_membern_IP_ 地址：端口

> 注意
>
> - 如果没有主机名，则显示对应的 IP 地址。
> - 空列表示未为该 NetScaler 实例配置相应的实体。

个人报告：您还可以下载和查看所有实例和实体的独立报告。例如，您可以仅下载负载平衡虚拟服务器、负载平衡服务或负载平衡服务组的报告。

NetScaler 控制台允许您立即下载报告。您还可以计划在每天、每周或每月的某个固定时间生成报告。

生成组合负载平衡报告

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 网络功能。
2. 单击生成报告。
3. 在打开的 生成报告 页面上，您有两个选项可以查看报告：

   a) 在“立即导出”选项卡上，选择“负载平衡”，然后单击“确定”。

   合并报告将下载到您的系统上。

   b) 选择 计划报告 以创建定期生成和导出报告的计划。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

      i. 选择 启用计划。

      ii. 循环 -从列表中选择“每日”、“每周”或“每 月”。

      > 注意
      >
      > 如果您选择每周定期，请确保您选择要计划报表的工作日。

      > 注意
      >
      > 如果选择 每月 循环，请确保输入月中的几天，值介于 1 到 31 之间。

      iii. 导出时间 -以 24 小时格式在小时：分钟中输入时间。

      iv. 电子邮件 -选中复选框，然后从列表中选择配置文件，或单击 添加 创建电子邮件配置文件。

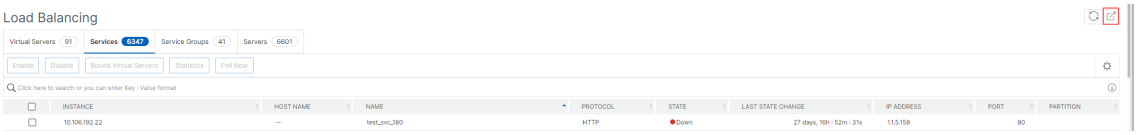
      v. **Slack** -选中 Slack 复选框，然后从列表框中选择配置文件，或单击 添加 创建松弛配置文件。

      vi. 单击“计划”以完成该过程。

生成单个负载平衡实体报告

您可以为与实例关联的特定类型的实体生成并导出单个报告。例如，假定这样一个场景：您要查看网络中所有负载平衡服务的列表。

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 网络功能 **>** 负载平衡 **>** 服务。
2. 在 服务 页面上，单击右上角的 导出 按钮。



如果要 在此时生成和查看报告，请选择“立即导出”选项卡。

> 注意
>
> 只能以邮件附件形式下载报告或导出报告。您无法在 NetScaler 控制台 GUI 上查看报告。

导出或计划网络功能报告的导出

January 29, 2024

您可以在 NetScaler 控制台中为选定的网络功能生成综合报告，例如负载平衡、内容交换、缓存重定向、全局服务器负载平衡 (GSLB)、认证和 NetScaler Gateway。使用此报告，您可以从高级视图了解网络中存在的实例、分区和相应的绑定实体（虚拟服务器、服务组和服务）之间的映射。您可以以.csv 文件格式导出这些报告。

报告显示以下虚拟服务器数据：

- NetScaler IP 地址
- 主机名
- 分区数据
- 虚拟服务器名称
- 虚拟服务器的类型
- 虚拟服务器
- 目标 LB 虚拟服务器

> 注意
>
> 对于内容交换和缓存重定向虚拟服务器，Target LB 虚拟服务器列列出了所有 LB 服务器，即默认服务器和基于策略的服务器。

- 服务名称
- 服务组名称

您可以计划按不同的间隔将这些报告导出到指定的电子邮件地址。有关如何设置电子邮件通知的信息，请参阅创建事件规则。

> 注意
>
> - 对于 GSLB 虚拟服务器，网络功能报告仅显示 GSLB 虚拟服务器和关联服务。
> - 对于内容切换和缓存重定向虚拟服务器，报告仅显示与关联负载平衡服务器的绑定。
> - 本报告中未列出 SSL 虚拟服务器，因为 NetScaler 控制台上没有单独的 SSL 虚拟服务器列表。
> - 生成新报告时，旧报告将自动从您的帐户中清除。

要导出和计划网络函数报告，请执行以下操作：

1. 导航到 基础结构 **>** 网络功能。
2. 在“网络函数”页面的右侧窗格中，单击页面右上角的“生成报告”。
3. 在 生成报告 页面上，您有以下 2 个选项：

   a) 选择“立即导出”选项卡，然后单击“确定”。

   报告将下载到您的系统。

   下图显示了网络函数报告的示例。

NetScaler IP Address	NetScaler HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	AppDB		Load Balancing	test_ssl[redacted]		svc2[redacted]	
[redacted]	AppDB		Load Balancing	testvser[redacted]		svc2[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p1_lb1#[redacted]		svc1#[redacted]	
[redacted]	AppDB	[redacted]	Load Balancing	p2_lb1#[redacted]		svc2#[redacted]	
[redacted]	NewBlrNS		Load Balancing	DAY_VS[redacted]		svc1C[redacted]	
[redacted]	NewBlrNS		Load Balancing	SSL_VS#[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	enable_[redacted]		svc1#[redacted]	
[redacted]	NewBlrNS		Load Balancing	test_ne[redacted]		svc1#[redacted]	

   b) 选择计划报告可创建定期生成和导出报告的计划。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

      i. 循环 -从下拉列表框中选择 每日、每周 或每 月。

      ii. 循环时间 -以 24 小时格式在“小时：分钟”中输入时间。

      iii. 电子邮件 -选中该复选框，然后从下拉列表框中选择配置文件，或单击 添加 以创建电子邮件配置文件。

      iv. **Slack** - 选中复选框，然后从下拉列表框中选择配置文件，或单击“添加”以创建电子邮件配置文件。

   单击 启用计划 以计划您的报告，然后单击 确定。通过单击 启用计划 复选框，您可以生成选定的报告。

网络报告

January 29, 2024

您可以通过在 NetScaler 控制台上监视网络报告来优化资源使用。您可能有包含许多部署在多个位置的应用程序的分布式部署。为确保应用程序获得最佳性能，您还部署了多个 Citrix Application Delivery Controller (NetScaler) 实例来实现负载平衡、内容切换或压缩流量。网络性能会影响应用程序性能。要继续保持应用程序的性能，必须定期监视网络性能并确保所有资源都得到最佳利用。

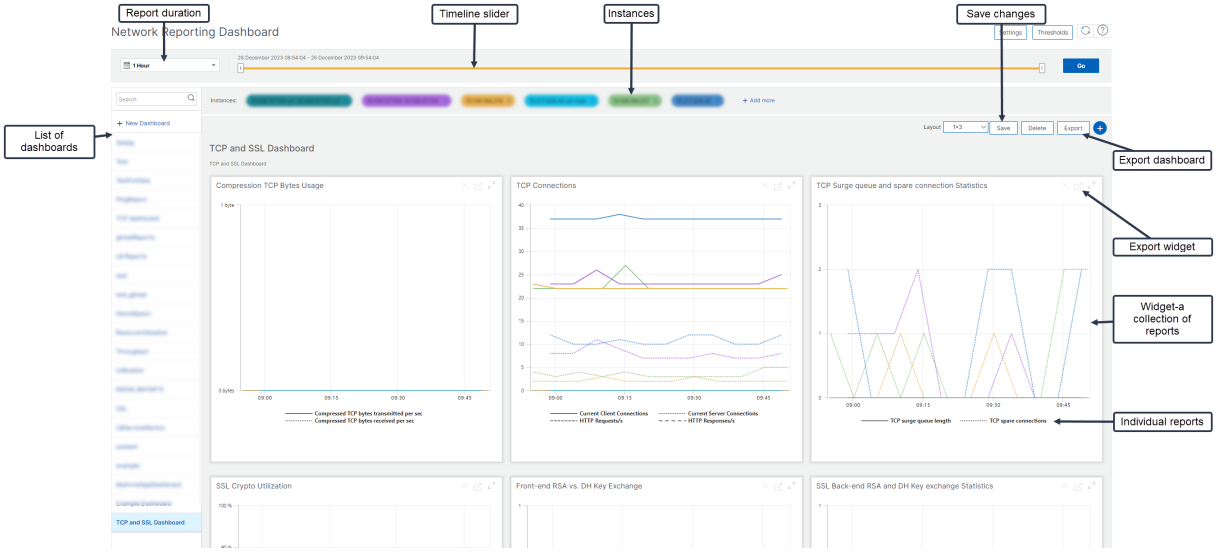
NetScaler 控制台允许您为全局级别的实例和实体（例如虚拟服务器和网络接口）生成报告。您可以为其生成报告的虚拟服务器如下所示：

- 负载平衡服务器、服务和服务组
- 内容交换服务器
- 缓存重定向服务器
- 全局服务负载平衡 (GSLB)
- 身份验证
- NetScaler Gateway

您可以在 NetScaler 控制台中为各种实例、虚拟服务器和其他实体创建多个控制板。

网络报告控制板

下图显示了控制板中的各种功能：



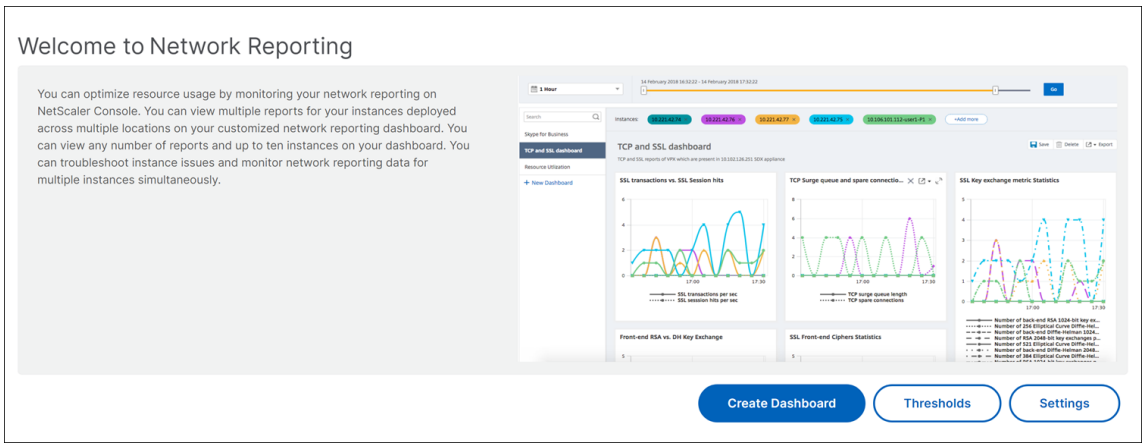
- 左侧面板列出了在 NetScaler 控制台中创建的所有定制控制板。您可以单击其中一个以查看控制面板所组成的各种报告。例如，TCP 和 SSL 控制板包含与 TCP 和 SSL 协议相关的各种报告。
- 您可以使用多个微件自定义每个控制板以显示各种报告。小组件表示控制板上的报表，即更多相关报表的集合。例如，压缩 TCP 字节使用情况报告包含每秒传输和接收的压缩 TCP 字节数的报告。
- 您可以显示一小时、一天、一周或一个月的报告。您可以使用时间轴滑块选项自定义在 NetScaler 控制台上生成报告的持续时间。
- 您可以通过单击“X”删除报告。您也可以将报告导出为.pdf、.jpeg、.png 或.csv 格式到您的系统。您还可以安排生成报告的时间和重复出现的时间。您还可以配置要向其发送报告的电子邮件通讯组列表。

- 控制板顶部的“实例”部分列出了生成报告的所有实例的 IP 地址。
- 您可以通过单击“X”删除实例，也可以向报告添加更多实例。但是，目前 NetScaler 控制台允许您查看 10 个实例的报告。
- 您还可以将整个控制板导出为.pdf、.jpeg、.png 或.csv 格式到您的系统。必须保存对控制板所做的任何更改。单击保存保存更改。

以下部分详细介绍了创建控制板、生成报表和导出报表的任务。

要查看或创建控制板，请执行以下操作：

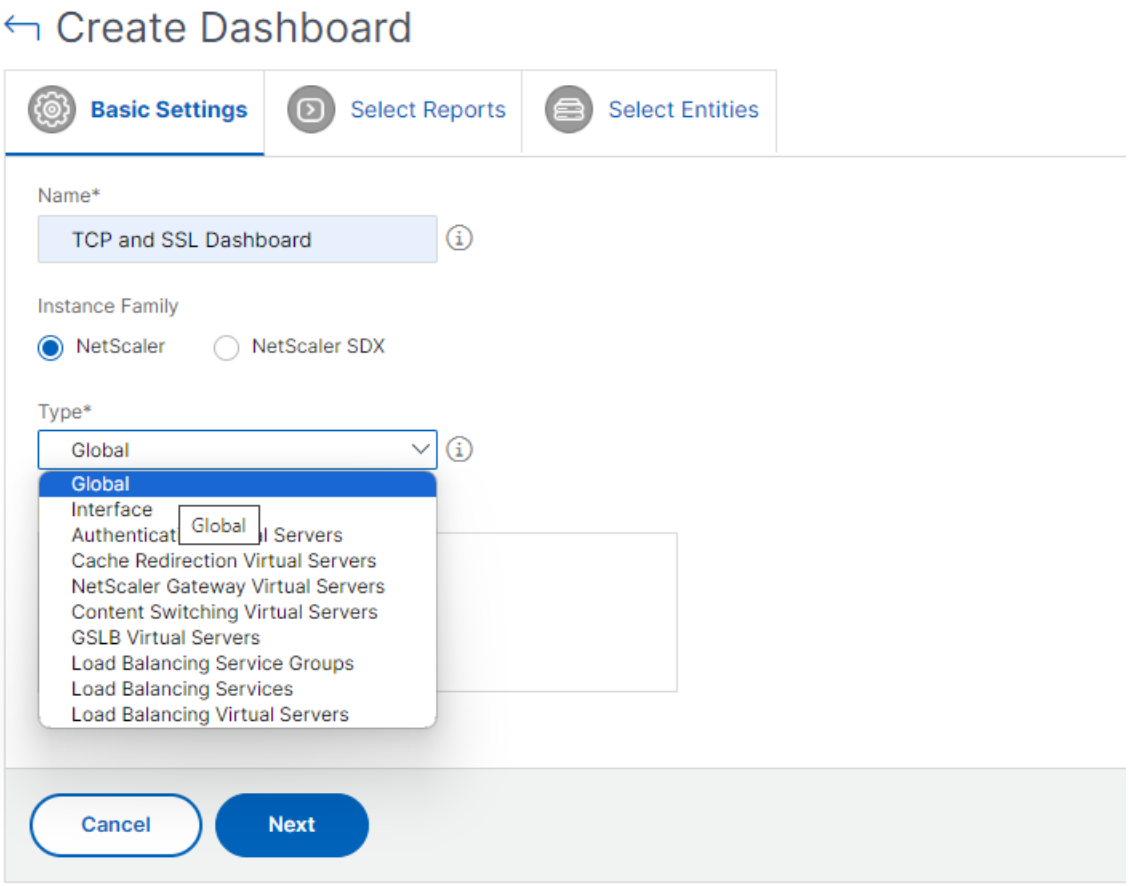
1. 在 NetScaler 控制台中，导航 到基础架构 **>** 网络报告。



2. 要查看现有控制板，请单击 查看控制板。“网络报表仪表 板 页将打开，您可以在其中查看所有控制板和报表小组件。

3. 要创建控制板，请单击“创建控制板”。

   “创建控制面板”页面打开。



4. 在“基本设置”选项卡中，输入以下详细信息：

   a) 名称。键入控制板的名称。

   b) 实例系列。选择实例类型——NetScaler 或 NetScaler SDX。

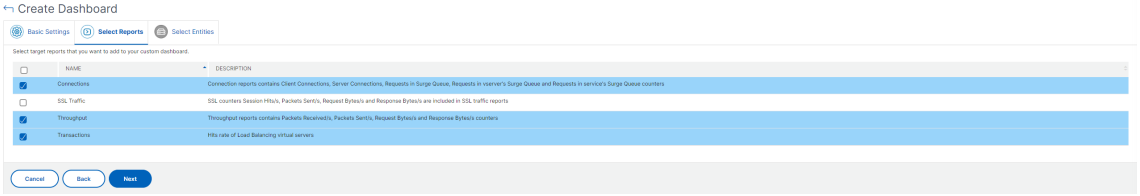
   <!–1. 实例系列。选择实例类型——NetScaler、Citrix SD-WAN 或 NetScaler SDX。–>

   a) 类型。选择要为其生成报告的实体类型。在此示例中，选择负载平衡虚拟服务器。

   b) 说明。为控制板键入有意义的描述。

5. 单击下一步。

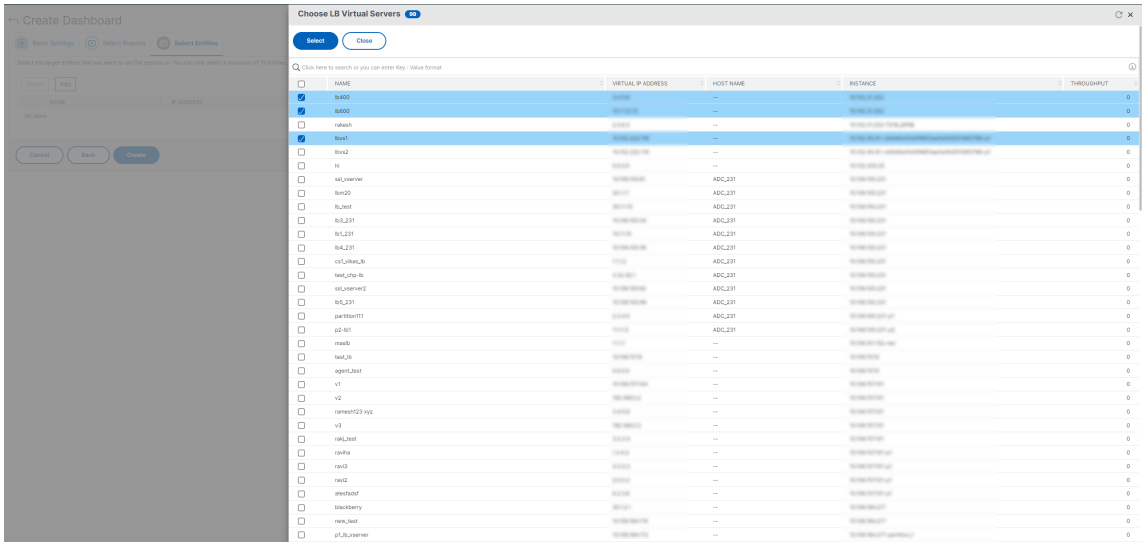
6. 在 选择报告 选项卡中，选择所需的报告。在此示例中，您可以选择事务、连接和吞吐量。单击下一步。



7. 在“选择实体”选项卡中，单击“添加”。

根据“基本设置”选项卡中选定的实体类型，将出现一个窗口，其中 包含 实体列表。在此示例中，将显示“选择 **LB** 虚拟服务器”窗口。

8. 选择要监视的实体。



9. 单击创建。

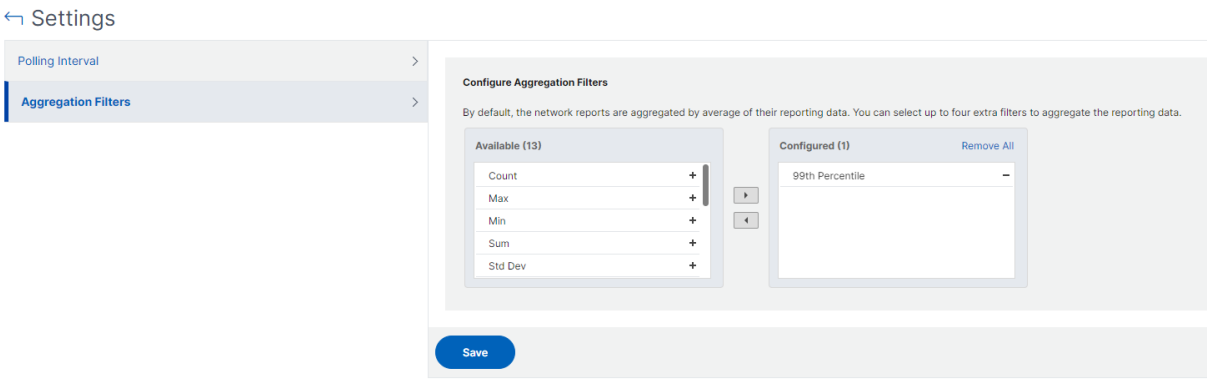
控制板已创建并显示您选择的所有报告。

> 注意
>
> 目前，无法保存您对图例或筛选器所做的任何更改。

通过应用聚合查看网络报告数据

您可以将聚合应用于网络性能数据，并在控制板上查看应用程序性能。您还可以根据自己的要求导出结果。使用这些应用于数据的聚合，您可以分析和检查所有资源是否得到最佳利用。导航到“网络” **>** “网络报告”，然后选择“持续时间 1 天或更晚”以获取“查看依据”选项。

在现有平均数据中，您可以通过从“查看 依据”列表中选择选项来应用聚合。应用聚合时，控制板中的每个指标的数据都会更新。单击 设置 并选择 聚合筛选器。



以下是您可以添加的聚合：

- 计数
- 最大
- 最小
- 求和
- Std 开发
- 差异
- 模式
- 中位数
- 第 25 个百分位数
- 第 75 个百分位
- 第 95 个百分位
- 99 个百分位数
- 第一个
- 最后一个

您最多可以向控制板添加 4 个聚合选项。添加聚合选项后，NetScaler 控制台大约需要 1 个小时才能为所选聚合选项生成报告。

导出网络报告

虽然您可以以.pdf、.png、.jpeg 或.csv 格式导出小组件报告，但只能以.pdf、.jpeg 或.png 格式导出整个控制板。

> 注意
>
> 如果您具有只读权限，则无法在 NetScaler 控制台中导出报告。您需要编辑权限才能在 NetScaler 控制台中创建文件并导出该文件。

要导出控制板报告，请执行以下操作：

1. 导航到 基础结构 **>** 网络报告
2. 单击“查看控制板”以查看您创建的所有控制板。
3. 在左窗格中，单击控制板。在此示例中，单击“控制板 **1**”。
4. 点击页面右上角的导出按钮。

5. 在“立即导出”选项卡下，选择所需的格式，然后单击“导出”。

   在 导出 页面上，您可以执行以下操作之一：

6. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
7. 选择 计划导出 选项卡。安排每天、每周或每月报告，并通过电子邮件或松弛消息发送报告。

   您可以安排定期导出 网络报告控制板 页面。例如，您可以设置一个选项，以便在特定时间的前一小时内每周生成控制板报告。然后，该报告每周生成一次，显示控制板的状态。该报告将覆盖时间和日期戳（如果由用户设置）。

> 注意
>
> - 如果选择“每周重复”，请选择要在哪个工作日发布报告。
> - 如果选择“每月重复”，请输入您希望安排报告的所有日期，以逗号分隔。

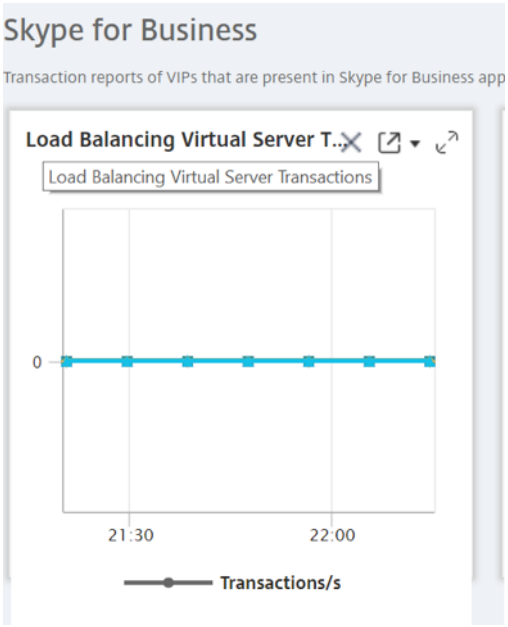
安排网络报告时，您可以通过在“主题”字段中输入文本字符串来自定义报告的标 题。在计划时间创建的报告的名称为此字符串。

例如，对于来自特定虚拟服务器的网络报告，可以键入主题为 “身份验证报告-10.106.118.120”，其中 10.106.118.120 是被监视虚拟服务器的 IP 地址。

> 注意
>
> 当前，此选项仅在您计划导出报告时可用。立即导出标题时，无法将标题添加到报表中。

要导出小组件报表，请执行以下操作：

1. 导航到 基础结构 **>** 网络报告。
2. 单击 查看控制板 以查看您已创建的所有控制板。
3. 在左窗格中，单击控制板。在此示例中，还单击 **Skype for Business**。
4. 选择一个小组件。例如，选择 负载平衡虚拟服务器事务。
5. 单击页面右上角的导出按钮
6. 在“立即导出”选项卡下，选择所需的格式，然后单击“导出”。



如何在 **NetScaler** 控制台上管理网络报告的阈值

要监视 NetScaler 实例的状态，可以在计数器上设置阈值并在超过阈值时接收通知。在 NetScaler 控制台上，您可以配置阈值并查看、编辑和删除阈值。

例如，当内容交换虚拟服务器的连接计数器达到指定值时，您可以收到电子邮件通知。您可以为特定实例类型定义阈值。您还可以从所选实例中选择要为特定计数器指标生成的报告。

当计数器的值超过或低于（由规则指定）阈值时，将生成具有指定严重性的事件以表示性能相关问题。计数器值恢复到您认为正常的值时，将清除事件。可以通过导航到 基础结构 **>** 事件 **>** 报告来查看这些事件。在“报告”页面上，您可以单击“按严重性划分的事件”圆环以按严重性查看事件。

您还可以将操作与阈值关联，例如在超过阈值时发送电子邮件或 SMS 消息。

要创建阈值，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 网络报告 **>** 阈值。在 **Thresholds**（阈值）下方单击 **Add**（添加）。
2. 在“创建阈值”页面上，指定以下详细信息：
   - 名称。阈值的名称。
   - 实例类型。一个 NetScaler 实例。
   - 报告名称。提供有关此阈值的信息的性能报告的名称。
3. 您还可以设置规则来指定何时生成或清除事件。您可以在“配置规则”部分下指定以下详细信息：
   - 指标。选择要为其设置阈值的指标。
   - 比较器。选择比较器以检查监视值是否大于或等于或小于或等于阈值。

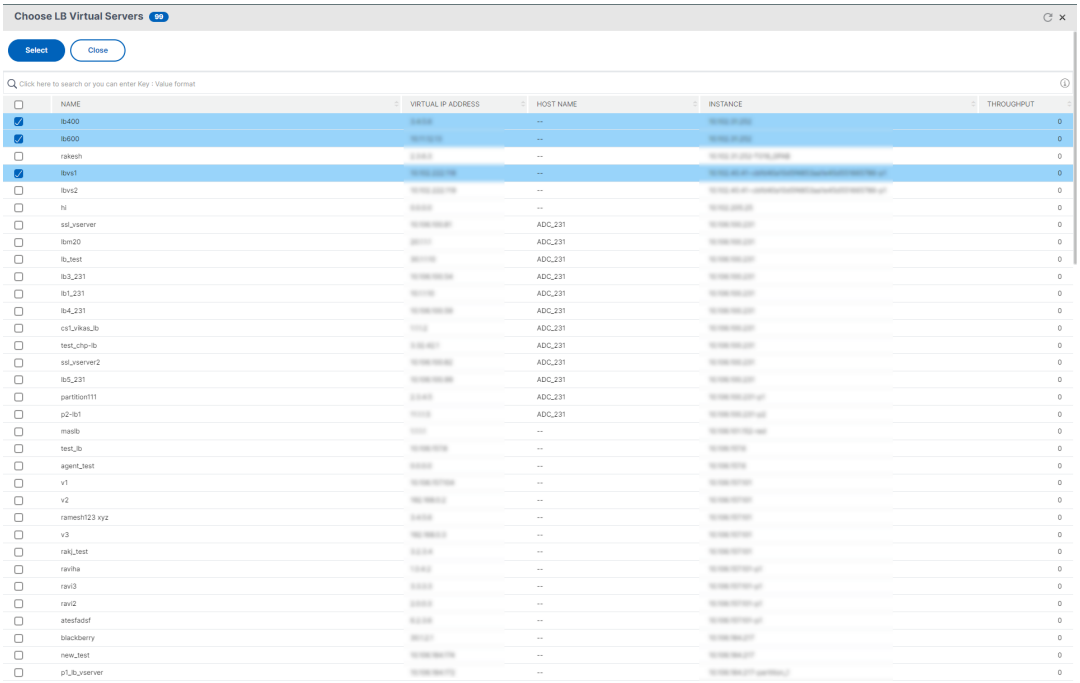
- 阈值。键入用于计算事件严重性的值。例如，您可能希望在当前客户端连接的监视值达到 80% 时生成事件严重性为严重的事件。在此情况下，键入 80 作为阈值。您可以通过导航到 基础结构 **>** 事件 **>** 报告来查看“严重严重性”事件。在“报告”页面上，您可以单击“按严重性划分的事件”圆环以按严重性查看事件。
- 清除值。键入指示何时清除该值的值。例如，您可能希望在监视的值达到 50% 时清除当前客户端连接阈值。在此情况下，键入 50 作为清除值。
- 事件严重性。选择要为阈值设置的安全级别。

4. 您可以选择使用阈值设置的实例和实体。在实例部分中，选择以下选项之一：

   - 所有实例。为所有实例设置了阈值。
   - 特定实例。阈值是为特定实例设置的。使用右箭头将实例从“可用”列表移至“已配置”列表。阈值是为已配置列表中的实例设置的。
   - 特定实体。阈值是为特定实体设置的。

     单击“添加”以选择实体。

     将出现一个窗口，其中包含实体列表，具体取决于报告名称字段中选定的报告类型。在此示例中，将显示“选择 **LB** 虚拟服务器”窗口。



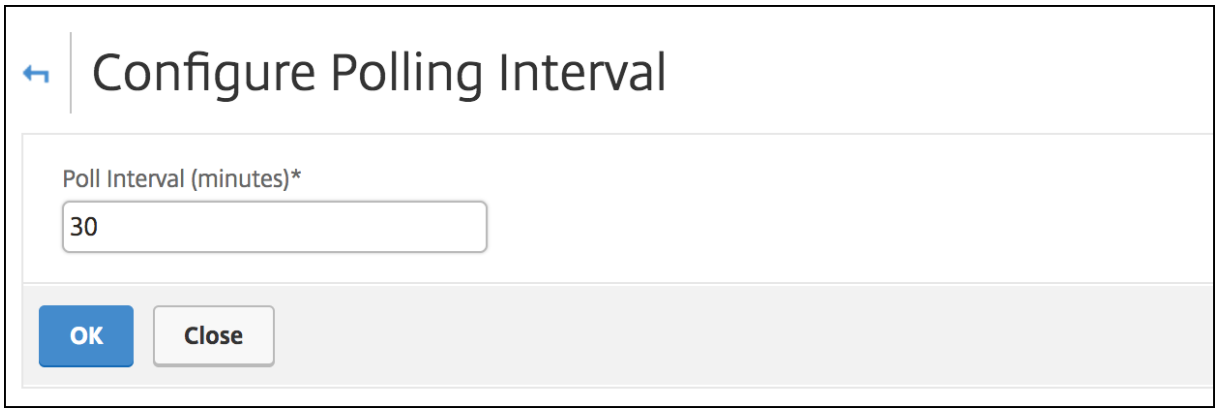
     选择要为其设置阈值的实体。单击 **Select**（选择）。所选实体显示在“实例”部分中。

5. 您可以选择在达到阈值时显示一条消息。在“事件消息”部分，在消息框中键入消息。NetScaler 控制台将监视值和阈值附加到此消息中。
6. 在通知设置部分中，选择启用阈值以启用阈值以生成警报。或者，您可以选择“通过电子邮件通知”，在达到阈值时通过电子邮件、Slack、ServiceNow 或 PagerDuty 等各种渠道接收通知。
7. 单击创建。

为网络报告设置性能轮询时间间隔

默认情况下，每 5 分钟 NITRO 调用收集一次性能数据用于网络报告。NetScaler 控制台检索计数器信息等实例统计信息，并根据每分钟、每小时、每天或每周进行汇总。可以在预定义的报告中查看此汇总数据。

要设置性能轮询间隔，请导航到 基础结构 **>** 网络报告，然后单击 配置轮询间隔。轮询时间间隔不能低于 5 分钟，也不能超过 60 分钟。



配置网络报告修剪设置

您可以在 NetScaler 控制台中配置网络报告数据的清除间隔。此间隔限制了存储在 NetScaler 控制台服务器数据库中的网络报告数据量。默认情况下，每 24 小时（01.00 小时）对报告历史数据的网络进行修剪。

> 注意
>
> 您可以指定的值不能超过 90 天或小于 1 天。

在 **AWS** 上预配 **NetScaler VPX** 实例

January 29, 2024

将应用程序迁移到云端时，作为应用程序一部分的组件会增加，变得更加分散，需要进行动态管理。

借助 AWS 上的 NetScaler VPX 实例，您可以将您的 L4-L7 网络堆栈无缝扩展到 AWS。借助 NetScaler VPX，AWS 成为您的本地 IT 基础设施的自然延伸。您可以在 AWS 上使用 NetScaler VPX 将云的弹性和灵活性与支持世界上最苛刻的网站和应用程序的相同优化、安全和控制功能相结合。

通过 NetScaler 控制台监视您的 NetScaler 实例，您可以了解应用程序的运行状况、性能和安全。您可以在混合多云环境中自动设置、部署和管理应用程序交付基础结构。

AWS 术语

以下部分简要介绍了本文档中使用的 AWS 术语：

术语	定义
Amazon Machine Image (AMI)	计算机映像，提供启动实例（云中的虚拟服务器）所需的信息。
弹性计算云 (EC2)	在云中提供安全、可调整大小的计算能力的 Web 服务。它旨在为开发人员简化 Web 规模的云计算。
弹性网络接口 (ENI)	可以附加到 VPC 中的实例的虚拟网络接口。
实例类型	Amazon EC2 提供了多种经过优化以符合不同用例的实例类型。实例类型包括 CPU、内存、存储和网络容量的各种组合，让您能够为您的应用程序灵活选择合适的资源组合。
身份识别和访问管理 (IAM) 角色	具有权限策略的 AWS 身份，这些策略确定该身份在 AWS 中可以执行哪些操作以及不能执行哪些操作。您可以使用 IAM 角色启用 EC2 实例上运行的应用程序以安全地访问 AWS 资源。
安全组	实例的一组指定的允许入站网络连接。
子网	EC2 实例可以附加到的 VPC 的一段 IP 地址范围。您可以根据安全和操作需求创建子网来对实例进行分组。
虚拟私有云 (VPC)	用于置备 AWS 云的逻辑隔离部分的 Web 服务，在此部分您可以在您定义的虚拟网络中启动 AWS 资源。

必备条件

本文档假定以下情况：

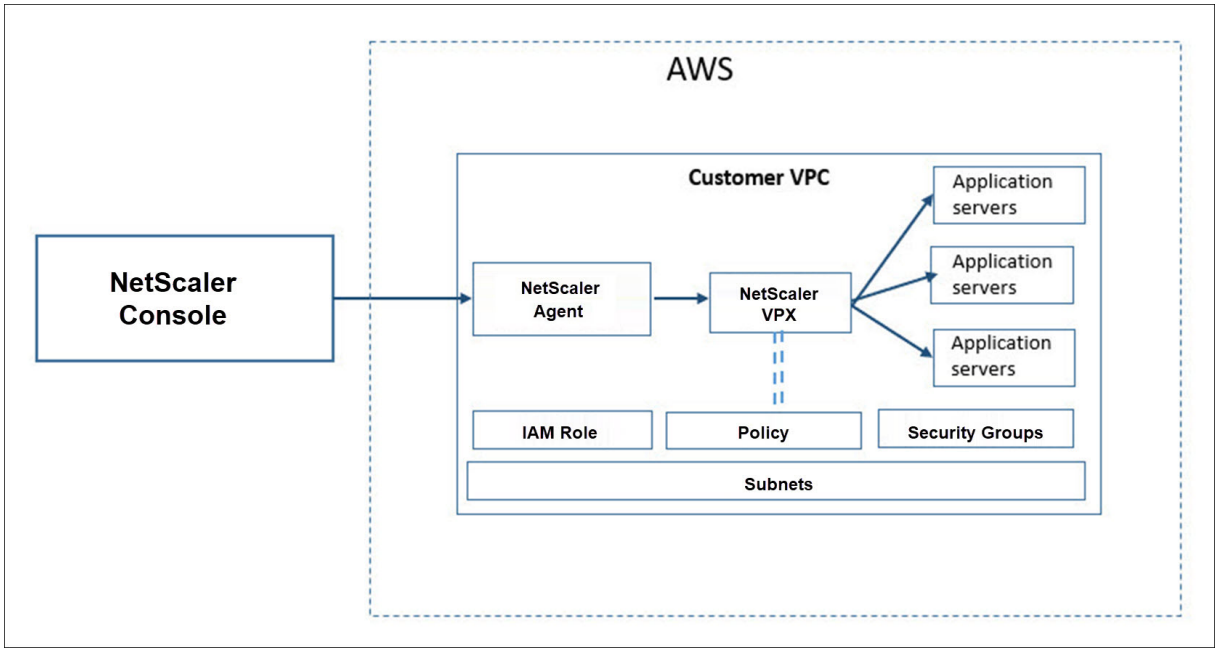
- 您拥有一个 AWS 帐户。
- 您已创建所需的 VPC 并选择了可用区。
- 您已在 AWS 中添加了代理。

有关如何创建帐户和其他任务的更多信息，请参阅 AWS 文档。

有关如何在 AWS 上安装代理的更多信息，请参见在 AWS 上 安装 NetScaler代理。

架构图

下图概述了 NetScaler 控制台如何与 AWS 连接以在 AWS 中预置 NetScaler VPX 实例。



配置任务

在 NetScaler 控制台中预置 NetScaler VPX 实例之前，在 AWS 上执行以下任务：

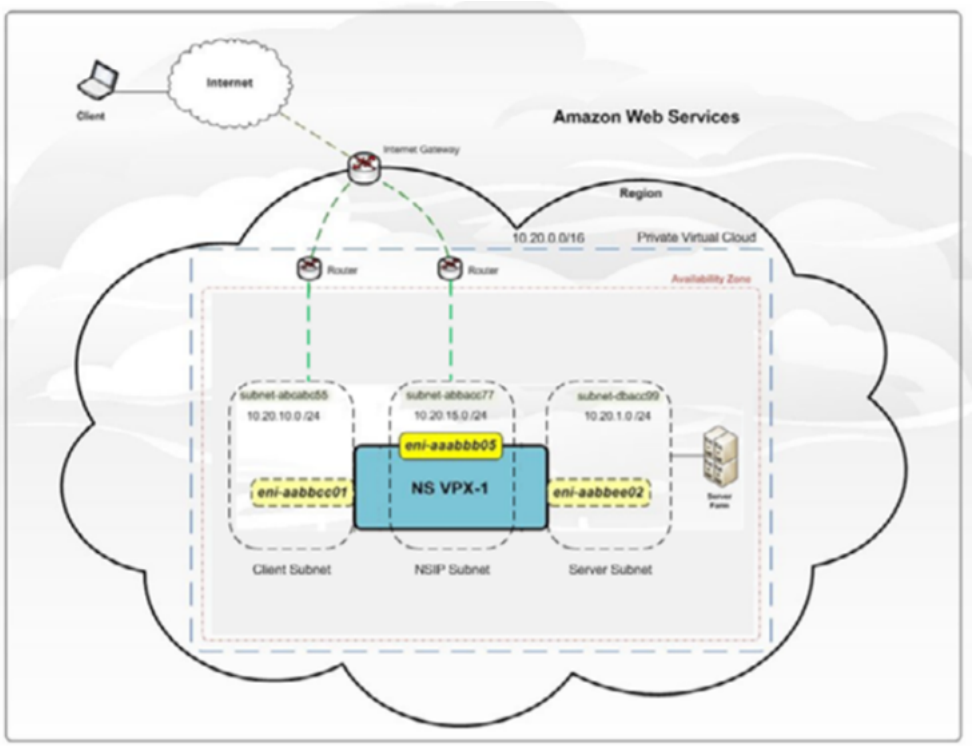
- 创建子网
- 创建安全组
- 创建 IAM 角色并定义策略

在 NetScaler 控制台上执行以下任务以在 AWS 上预置实例：

- 创建网站
- 在 AWS 上配置 NetScaler VPX 实例

创建子网

在您的 VPC 中创建三个子网。在 VPC 中配置 NetScaler VPX 实例所需的三个子网是管理、客户端和服务器。在 VPC 中为每个子网定义的范围内指定 IPv4 CIDR 块。指定希望子网驻留的可用区。在同一可用区域中创建所有三个子网。下图说明了在您的区域中创建的三个子网及其与客户端系统的连接。



有关 VPC 和子网的更多信息，请参阅 VPC 和子网。

创建安全组

创建安全组以控制 NetScaler VPX 实例中的入站和出站流量。安全组充当您的实例的虚拟防火墙。在实例级别而不是子网级别创建安全组。可以将 VPC 中子网中的每个实例分配给一组不同的安全组。为每个安全组添加规则，以控制通过客户端子网传递到实例的入站流量。您还可以添加一组单独的规则来控制通过服务器子网到达应用程序服务器的出站流量。尽管您可以为实例使用默认安全组，但您可能需要创建您的组。创建三个安全组-每个子网一个。为要控制的传入和传出流量创建规则。您可以根据需要添加多个规则。

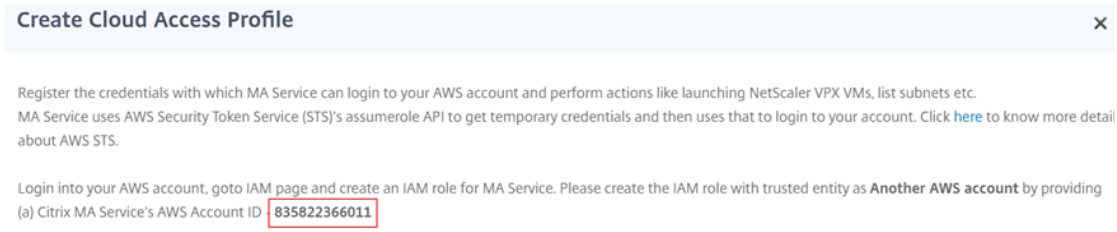
有关安全组的更多信息，请参阅 您的 VPC 的安全组。

创建 **IAM** 角色并定义策略

创建 IAM 角色，以便您可以在用户与 Citrix 受信任的 AWS 帐户之间建立信任关系，并创建具有 Citrix 权限的策略。

1. 在 AWS 中，单击“服务”。在左侧导航窗格中，选择 **IAM >** 角色，然后单击 创建角色。
2. 您正在将您的 AWS 帐户与 NetScaler 控制台中的 AWS 帐户关联起来。因此，选择 另一个 **AWS** 帐户 以允许 NetScaler 控制台在您的 AWS 帐户中执行操作。

   输入 12 位数的 NetScaler 控制台 AWS 帐户 ID。Citrix ID 为 835822366011。创建云访问配置文件时，您还可以在 NetScaler 控制台中找到 Citrix ID。



3. 启用 要求外部 **ID** 连接到第三方帐户”。您可以通过要求使用可选的外部标识符来提高角色的安全性。键入可以是任何字符的组合的 ID。
4. 单击权限。
5. 在 附加权限策 略页面中，单击 创建策略。
6. 您可以在可视化编辑器中或使用 JSON 创建和编辑策略。

   以下框中提供了 Citrix 的权限列表：

```
{

"Version": "2012-10-17",
"Statement":
[
    {

          "Effect": "Allow",
         "Action": [
             "ec2:DescribeInstances",
             "ec2:DescribeImageAttribute",
             "ec2:DescribeInstanceAttribute",
             "ec2:DescribeRegions",
             "ec2:DescribeDhcpOptions",
             "ec2:DescribeSecurityGroups",
             "ec2:DescribeHosts",
             "ec2:DescribeImages",
             "ec2:DescribeVpcs",
             "ec2:DescribeSubnets",
             "ec2:DescribeNetworkInterfaces",
             "ec2:DescribeAvailabilityZones",
             "ec2:DescribeNetworkInterfaceAttribute",
             "ec2:DescribeInstanceStatus",
             "ec2:DescribeAddresses",
             "ec2:DescribeKeyPairs",
             "ec2:DescribeTags",
             "ec2:DescribeVolumeStatus",
             "ec2:DescribeVolumes",
             "ec2:DescribeVolumeAttribute",
             "ec2:CreateTags",
             "ec2:DeleteTags",
             "ec2:CreateKeyPair",
             "ec2:DeleteKeyPair",
             "ec2:ResetInstanceAttribute",
```



```
                "ec2:RunScheduledInstances",
                "ec2:ReportInstanceStatus",
                "ec2:StartInstances",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:UnmonitorInstances",
                "ec2:MonitorInstances",
                "ec2:RebootInstances",
                "ec2:TerminateInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses",
                "ec2:CreateNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:DetachNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:ResetNetworkInterfaceAttribute",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:AssociateAddress",
                "ec2:AllocateAddress",
                "ec2:ReleaseAddress",
                "ec2:DisassociateAddress",
                "ec2:GetConsoleOutput"
            ],
                "Resource": "*"
        }

    ]
     }
```

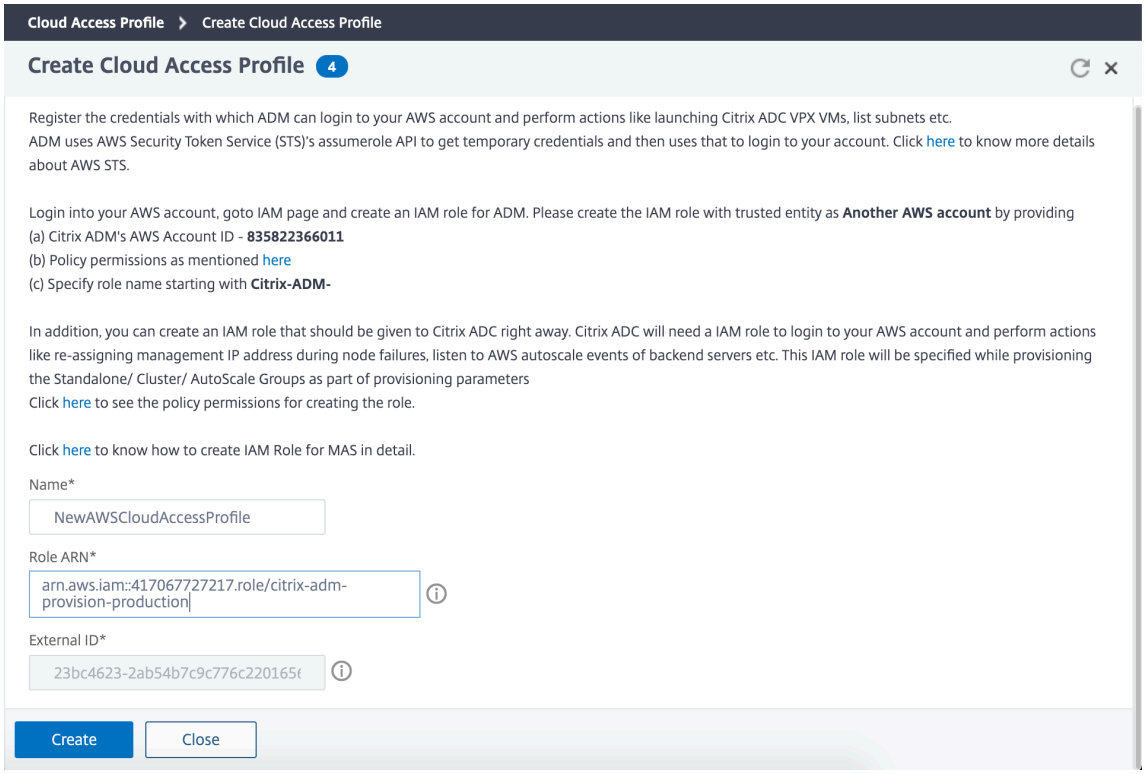
7. 复制并粘贴 JSON 选项卡中的权限列表，然后单击 查看策略。
8. 在“查看策略”页面中，键入策略的名称，输入描述，然后单击“创建策略”。

在 **NetScaler** 控制台中创建站点

在 NetScaler 控制台中创建一个站点，然后添加与您的 AWS 角色关联的 VPC 的详细信息。

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 站点。
2. 单击添加。
3. 选择服务类型为 AWS 并启用“使用现有 **VPC** 作为站点”。
4. 选择云访问配置文件。
5. 如果字段中不存在云访问配置文件，请单击“添加”以创建配置文件。
    a) 在 创建云访问配置文件 页面中，键入您要用来访问 AWS 的配置文件的名称。
    b) 键入与您在 AWS 中创建的角色相关联的 ARN。

c) 键入您在 AWS 中创建身份和访问管理 (IAM) 角色时提供的外部 ID。请参阅创建 IAM 角色和定义策略任务中的步骤 4。确保您在 AWS 中指定的 IAM 角色名称以“Citrix-ADM-”开头并正确显示在角色 ARN 中。



与您在 AWS 中的 IAM 角色关联的 VPC 的详细信息，例如区域、VPC ID、名称和 CIDR 区块，将导入到 NetScaler 控制台中。

6. 键入站点的名称。
7. 单击创建。

在 **AWS** 上配置 **NetScaler VPX**

使用您之前创建的网站在 AWS 上配置 NetScaler VPX 实例。提供代理详细信息以配置绑定到该代理的实例。

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例 **> NetScaler**。
2. 在 **VPX** 选项卡中，单击 配置。

   此选项显示 在云上置备 **NetScaler VPX** 页面。
3. 选择 **Amazon Web Services (AWS)** ，然后单击 下一步。
4. 在“基本参数”选项卡中，

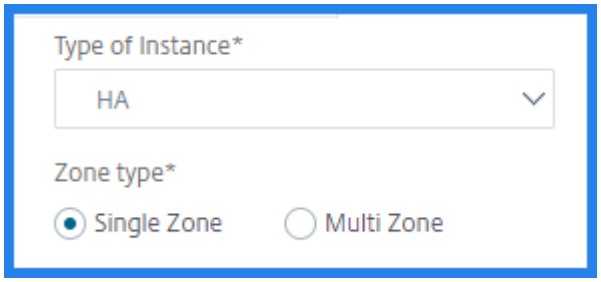
   a) 从列表 中选择实例类型。

   - 独立：此选项在 AWS 上配置一个独立的 NetScaler VPX 实例。

- **HA**：此选项在 AWS 上配置高可用性 NetScaler VPX 实例。

  要在同一区域中配置 NetScaler VPX 实例，请选择“区域类型”下的“单区域”选项。

  要跨多个区域置备 NetScaler VPX 实例，请选择“区域 类型”下的多区 ** 域”选项。在“预配参数 **”选项卡中，确保为在 AWS 上创建的每个区域指定网络详细信息。



b) 指定 NetScaler VPX 实例的名称。

c) 在站点中，选择您之前创建的站点。

d) 在 代理中，选择为管理 NetScaler VPX 实例而创建的代理。

e) 在云访问配置文件中，选择在站点创建过程中创建的云访问配置文件。

f) 在 设备配置文件中，选择要提供身份验证的配置文件。

   当需要登录到 NetScaler VPX 实例时，NetScaler 控制台会使用设备配置文件。

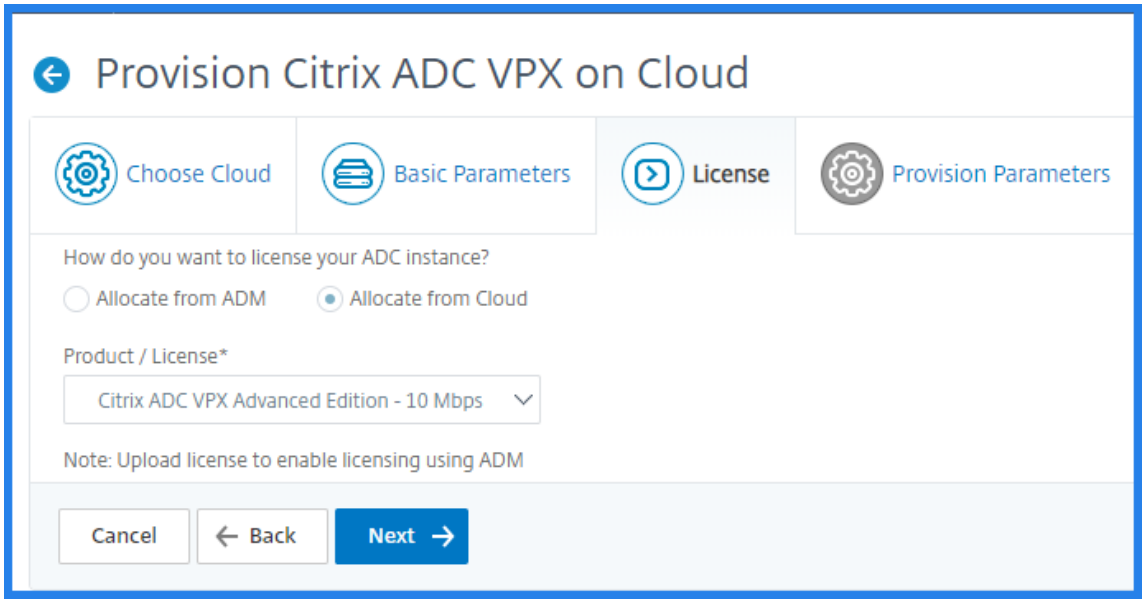
g) 单击下一步。

5. 在“许可”标签中，选择以下模式之一将许可应用于 NetScaler 实例：

   - 使用 **NetScaler** 控制台：您要预置的实例会从 NetScaler 控制台中检出许可。
   - 使用 **AWS** 云：“从云端分配”选项使用 AWS 市场上提供的 NetScaler 产品许可证。您要预置的实例使用市场中的许可证。

     如果您选择使用 AWS 市场中的许可证，请在“预配参数”选项卡中指定产品或许可证。

有关更多信息，请参阅 许可要求。



6. 在“许可”标签中，如果您选择“从 **NetScaler** 控制台分配”，请指定以下内容：

   - 许可证类型-选择带宽或虚拟 CPU 许可证：

     带宽许可证：您可以从“带 宽许可证类型”列表中选择以下选项之一：

     - 池容量：指定要分配给实例的容量。

       NetScaler 实例从公共池中检出一个实例许可，并且仅指定了多少带宽。

     - **VPX** 许可：配置 NetScaler VPX 实例时，该实例将从 NetScaler 控制台签出许可。

     虚拟 **CPU** 许可证：预配置的 NetScaler VPX 实例根据实例中运行的 CPU 数量签出许可证。

     > 注
     >
     > 意：当预置的实例被移除或销毁时，应用的许可将返回到 NetScaler 控制台许可池。这些许可证可以重复用于预置新实例。

   a) 在 许可证版本中，选择许可证版本。NetScaler 控制台使用指定的版本来配置实例。

7. 单击下一步。

8. 在“预配参数”选项卡中，

   a) 选择在 AWS 中创建的 **Citrix IAM** 角色。IAM 角色是一种 AWS 身份，其权限策略可确定身份在 AWS 中可以执行和不能执行的操作。

   b) 在“产品”字段中，选择要预置的 NetScaler 产品版本。

   c) 从实例类型列表中选择 EC2 实例类型。

   此列表显示所选 NetScaler 实例支持的 AMI 实例类型。

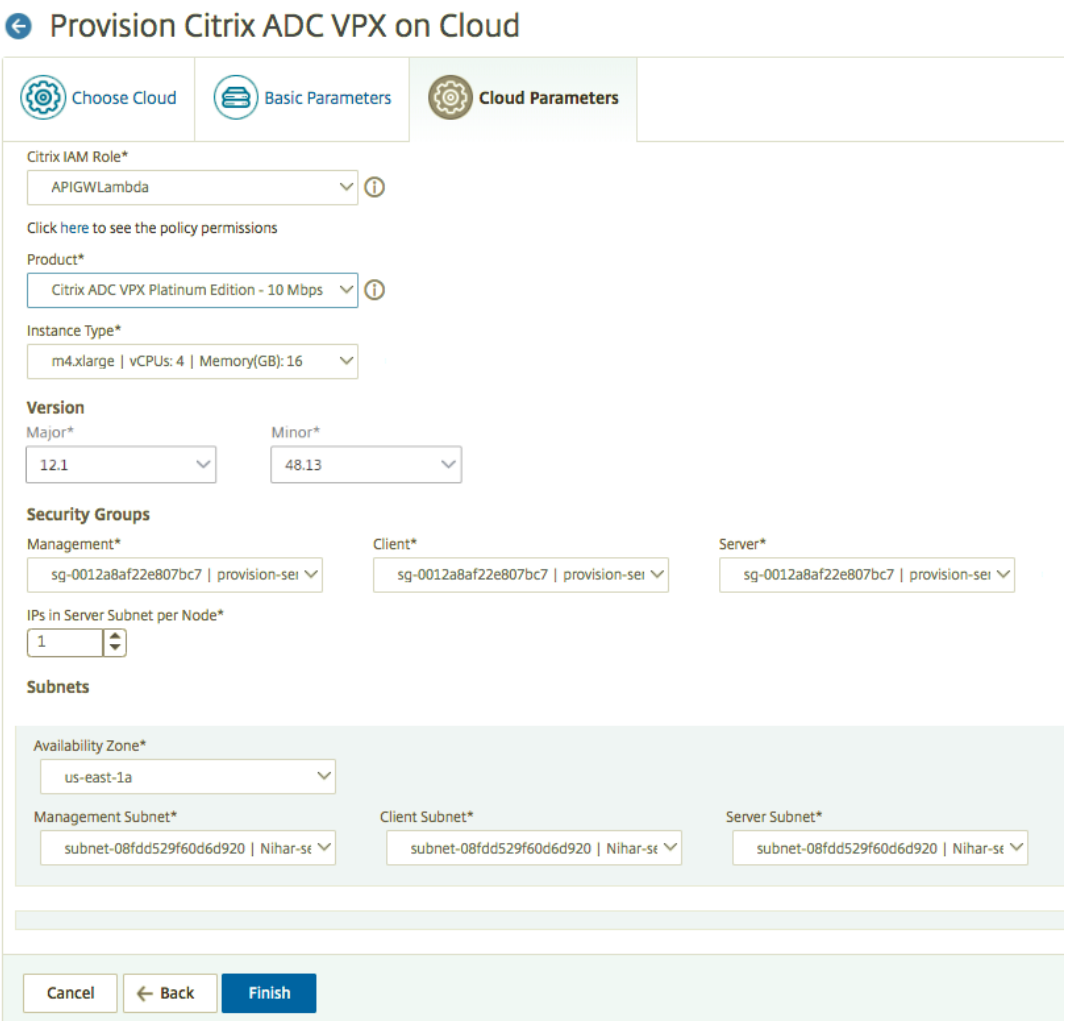
   d) 选择要预置的 NetScaler 版本。选择 NetScaler 的主要 和 次要 版本。

e) 在 安全组中，选择您在虚拟网络中创建的管理、客户端和服务器安全组。

f) 在 每个节点的服务器子网中的 IP 中，选择安全组每个节点的服务器子网中的 IP 地址数。

g) 在 子网中，为在 AWS 中创建的每个区域选择管理、客户端和服务器子网。您也可以从 可用区列表中选择区域。

h) 单击完成。



NetScaler VPX 实例现在已在 AWS 上预配置。

> 注
>
> 意目前，NetScaler 控制台不支持从 AWS 取消预配 NetScaler 实例。

查看 **AWS** 中预配置的 **NetScaler VPX**

1. 在 AWS 主页中，导航到 服务，然后单击 **EC2**。
2. 在 资源 页面上，单击 正在运行的实例。

3. 您可以查看 AWS 中预配置的 NetScaler VPX。

NetScaler VPX 实例的名称与您在 NetScaler 控制台中预置实例时提供的名称相同。

查看在 **NetScaler** 控制台中配置的 **NetScaler VPX**

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 实例 **> NetScaler**。
2. 选择 **NetScaler VPX** 选项卡。
3. 此处列出了在 AWS 中预配置的 NetScaler VPX 实例。

NetScaler App Delivery and Security 服务自助管理权限

January 29, 2024

NetScaler App Delivery and Security 服务自助管理是使用共用许可的新方式，在许可和容量管理方面实现了高度自动化。客户无需手动管理许可证，在混合多云环境中灵活管理容量需求。

> 先决条件
>
> 确保满足以下先决条件：
>
> - 确保您已在 NetScaler 控制台服务中注册了 NetScaler 代理
> - 支持的 NetScaler 版本如下：
>   - 版本 13.0：使用 13.0-88.12 或更高版本
>   - 版本 13.1：使用 13.1-30.x 或更高版本
> - 您使用的是 NetScaler 代理 13.1-32.x 或更高版本

作为 NetScaler App Delivery and Service 自助管理功能的一部分，一旦客户在 NetScaler 控制台服务上购买并创建了 NetScaler 代理，许可信息就会自动上载到 NetScaler 控制台服务。作为 NetScaler 控制台基础架构的一部分，许可直接下载到许可服务器代理 (LSA) 或 vPC/数据中心中的代理。

> 注意
>
> NetScaler App Delivery and Security 自助管理服务仅在 NetScaler 控制台服务上可用。

NetScaler 控制台可以托管现有的 Pooled 和 NetScaler App Delivery and Security Service 自助管理权限。要使用所需的许可证，请在 NetScaler 设备上配置许可证服务器，然后从相应的池中签出或分配容量。

NetScaler App Delivery and Security 服务自助管理具有以下功能：

- 提供标准版、高级版和高级版

- NetScaler App Delivery and Security Citrix 管理的高级版权限在第一年为每个自助管理入门池提供 100TB + 800 万 DNS 查询
- 初学者池包括每 1 Gbps 1 个 VIP 或每购买 1 个 vCPU 1 个 VIP。其他 VIP 可以作为附加组件购买

有关可用的 NetScaler App Delivery and Security 服务自助管理权限的更多信息，请导航到基础架构 **>** 自助管理。

您可以通过以下方式在 NetScaler 上配置许可证服务器的 IP 地址：

- 使用 CLI。有关更多信息，请参阅 使用 CLI 配置自管理池许可证
- 使用图形用户界面。有关更多信息，请参阅 使用 GUI 配置自管理池许可证

客户还可以在 NetScalerConsole 服务上跟踪许可到期和使用情况等信息。

为 **NetScaler** 实例分配 **NetScaler App Delivery and Service** 自助管理容量

January 29, 2024

您可以通过两种方式分配 NetScaler App Delivery and Security 服务自助管理权限和容量：

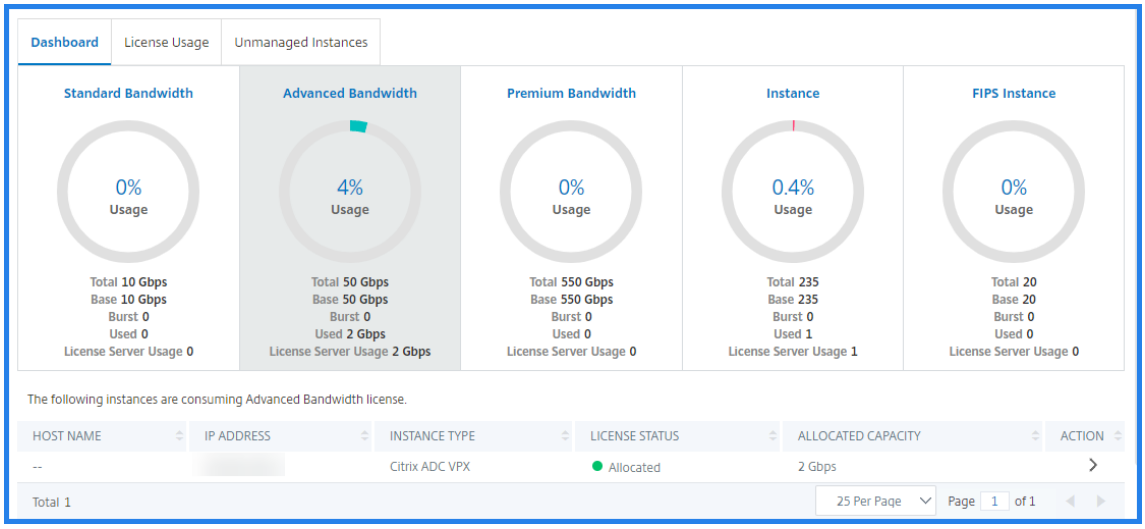
- 使用 NetScaler 实例
- 如果 NetScaler 由 ADM 管理，则使用 ADM。

要从 NetScaler 控制台 GUI 中分配 NetScaler App Delivery and Security Service 自助管理容量，请执行以下操作：

1. 登录 NetScaler 控制台。
2. 导航到 基础结构 **>** 自我管理 **>** 带宽许可证 **>** 自管理池。
3. 单击要管理的许可证池-标准版、高级版或高级版。

   > 注意：
   >
   > “分配的容量”字段不会立即反映更改的带宽。带宽更改在 NetScaler 热重启后生效。
   >
   > 在分配详细信息中，当您更改实例的带宽分配时，“已请求”和“已应用”字段将更新。

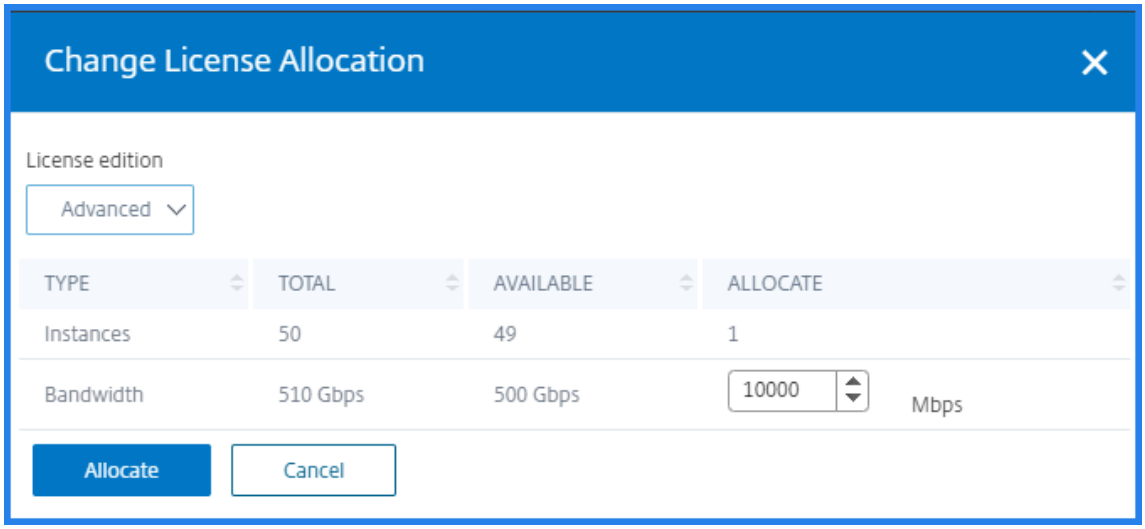
4. 单击 ** 按钮，从可用实例列表中选择 NetScaler 实例。



许可证状态列显示相应的权利分配状态消息。

> 注
>
> 意："非托管实例"选项卡显示已发现但未在 NetScaler 控制台中管理的实例。
>
> 
>

5. 单击"更改分配"或"发布分配"以修改许可证分配。
6. 将出现一个弹出窗口，其中包含许可证服务器中的可用许可证。
7. 通过设置分配列表选项来选择实例的带宽或实例分配。做出选择后，单击"分配"。
8. 您也可以从"更改许可证分配"窗口的列表选项中更改分配的许可证版本。

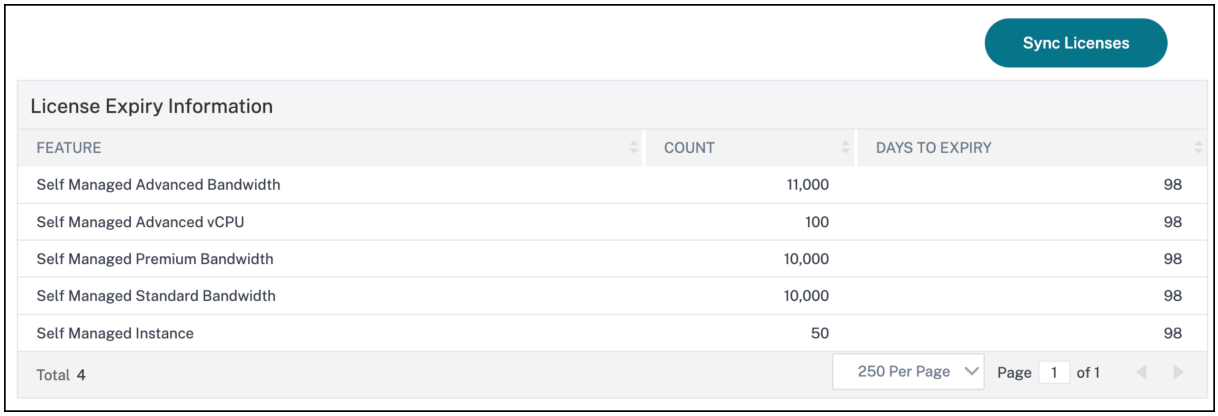


> 注意
>
> 如果您更改了许可版本，请热重启实例。

查看 **NetScaler App Delivery and Security** 服务自助管理授权信息

January 29, 2024

您可以导航到基础架构 **>** 自我管理，查看 NetScaler 控制台上提供的 NetScaler App Delivery and Security Service 自助管理权限



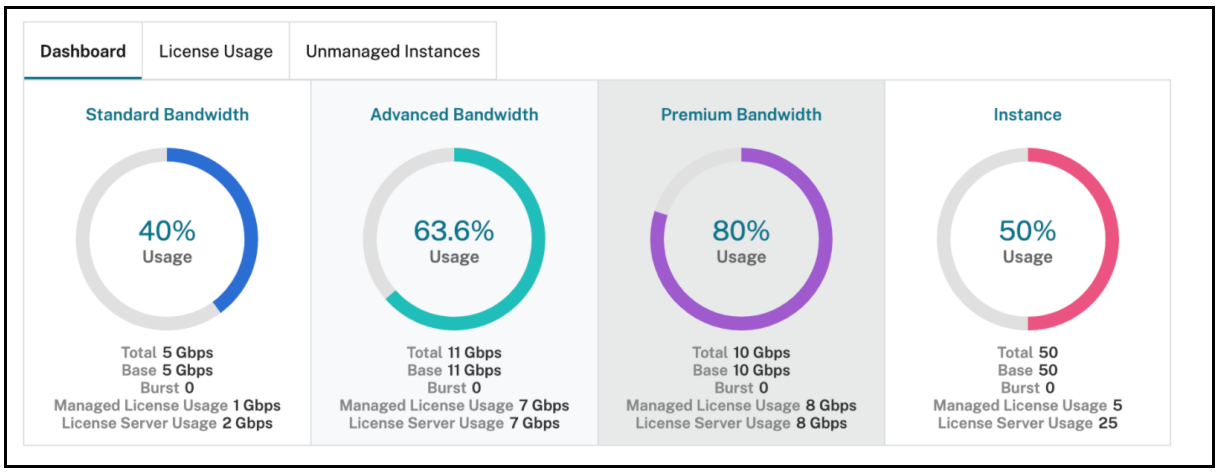
控制面板显示有关 NetScaler App Delivery and Security 服务自助管理授权的信息。如果授权信息未显示在控制面板上，或者授权信息的添加出现延迟，请单击“同步许可证”按钮，将显示可用的带宽池、计数和到期信息。

有关配置许可证到期检查的更多信息，请参阅 配置许可证到期检查。

在 许可证到期信息 部分，您可以查看即将到期的许可证的详细信息

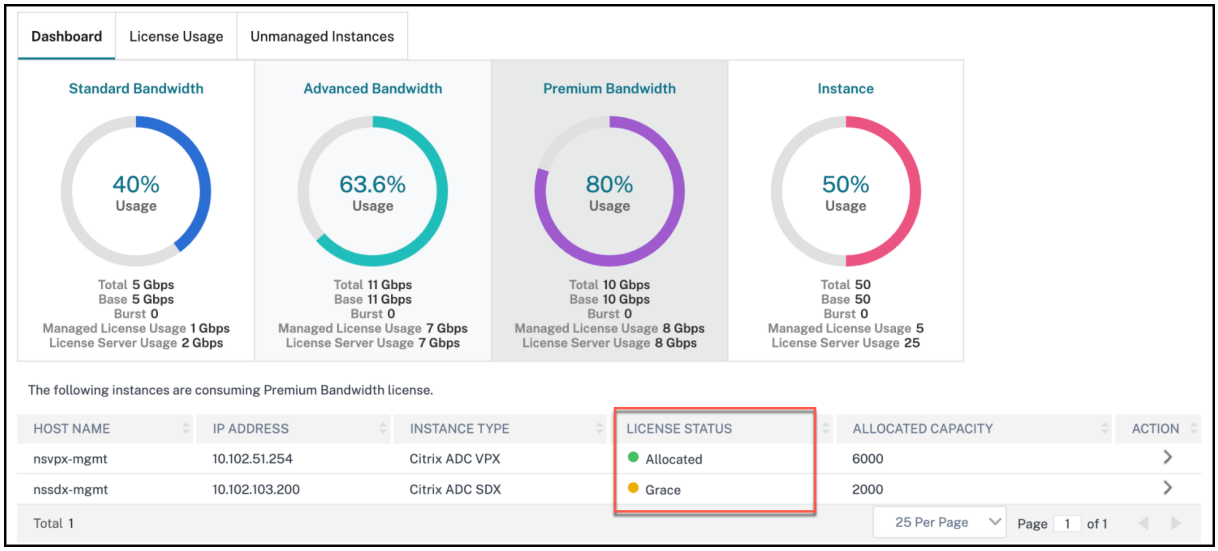
- 功能 -即将到期的许可证类型。
- 计数 -将受影响的虚拟服务器或实例的数量。
- 到期天 数-许可证到期前的天数。

要查看不同许可证版本的可用池，请导航到 基础结构 **>** 自管理 **>** 带宽许可证 **>** 自管理池



检查许可证使用情况

如果您已将 NetScaler 控制台配置为 NetScaler 池容量许可的许可服务器，则可以使用 NetScaler 控制台 GUI 来检查许可状态。导航到 基础结构 **>** 自我管理 **>** 池容量 **>** 许可证使用情况。



有关许可证状态类型及其含义的更多信息，请参阅 检查许可证状态。

管理服务图的 **Kubernetes** 群集

January 29, 2024

Kubernetes (K8s) 是一个开源容器调配平台，可自动部署、扩展和管理云原生应用。

> 注意
>
> - 使用 Kubernetes 版本 1.14—1.23，NetScaler 控制台支持 Service Graph 的群集可见性。

您可以在 NetScaler 控制台中指定 Kubernetes 集成的以下方面：

- 群集—您可以注册或取消注册 Kubernetes 群集，NetScaler 控制台会监视其中的所有微服务并填充服务图。在 NetScaler 控制台中注册群集时，请指定 Kubernetes API 服务器信息。然后，选择一个可以访问 Kubernetes 群集的代理。

开始之前的准备工作

要在 Kubernetes 群集上监视和可视化您的微服务并开始使用 Service Graph，请确保您有：

- 库贝内特斯群集到位。
- 安装并配置该代理以启用 NetScaler 控制台与 Kubernetes 群集或托管实例之间的通信。您可以使用数据中心或云中存在的托管实例。
- 在 NetScaler 控制台中注册的 Kubernetes 群集。

配置 **NetScaler** 代理以向 **Kubernetes** 群集注册

要启用 Kubernetes 群集和 NetScaler 控制台之间的通信，必须安装和配置代理。您可以在以下平台上部署代理：

- 虚拟机管理程序（ESX、XenServer、KVM、Hyper-V）
- 公有云服务（例如 Microsoft Azure、AWS）

按照 步骤 配置代理。

> 注意
>
> 如果已经部署了现有代理，您也可以使用该代理。

使用密钥令牌配置 **NetScaler** 控制台以管理 **Kubernetes** 群集

为了让 NetScaler 控制台能够接收来自 Kubernetes 的事件，您需要在 Kubernetes for NetScaler 控制台中创建一个服务帐户。此外，使用群集中必要的 RBAC 权限配置服务帐户。

1. 为 NetScaler 控制台创建服务帐户。例如，服务帐户名称可以是`citrixadm-sa`。要创建服务帐户，请参阅 使用多个服务帐户。
2. 使 `cluster-admin`用 角色绑定 NetScaler 控制台帐户。此绑定将 `ClusterRole` 整个群集中的授予服务帐户。以下是将 `cluster-admin` 角色绑定到服务帐户的示例命令。


```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
    =cluster-admin --serviceaccount=default:citrixadm-sa
```

将 NetScaler 控制台帐户绑定到角色后cluster-admin，该服务帐号具有群集范围的访问权限。有关更多信息，请参阅 kubectl 创建 clusterrolebinding。

3. 从创建的服务帐户获取令牌。

   例如，运行以下命令查看 citrixadm-sa 服务帐户的令牌：

```
kubectl describe sa citrixadm-sa
```

4. 运行以下命令获取令牌的密钥字符串：

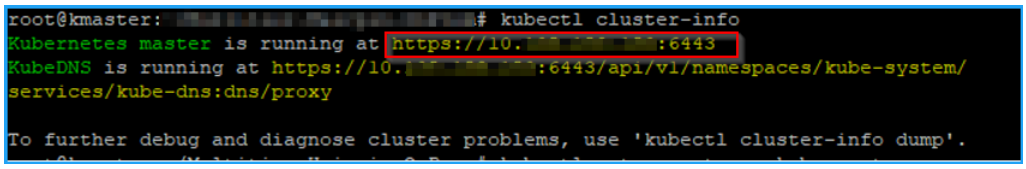
```
kubectl describe secret <token-name>
```

在 NetScaler 控制台中添加 Kubernetes 群集

配置代理和配置静态路由后，必须在 NetScaler 控制台中注册 Kubernetes 群集。

要注册 Kubernetes 群集，请执行以下操作：

1. 使用管理员凭据登录 NetScaler 控制台。
2. 导航到调配 > **Kubernetes** > 群集。
   屏幕上将显示“群集”页面。
3. 单击添加。
4. 在“添加群集”页中，指定以下参数：
   a) 名称 -指定您选择的名称。
   b) **API** 服务器 **URL** -您可以从 Kubernetes 主节点获取 API 服务器 URL 的详细信息。
      i. 在 Kubernetes 主节点上，运行命令 kubectl cluster-info。



      ii. 输入显示的 **Kubernetes** 主服务器正在运行的 URL。
   c) 认证令牌-指定在 配置 NetScaler 控制台以管理 Kubernetes 群集时获得的认证令牌字符串。验证令牌是验证 Kubernetes 群集和 NetScaler 控制台之间通信的访问权限所必需的。要生成身份验证令牌，请执行以下操作：
      i. 在 Kubernetes 主节点上，运行以下命令：

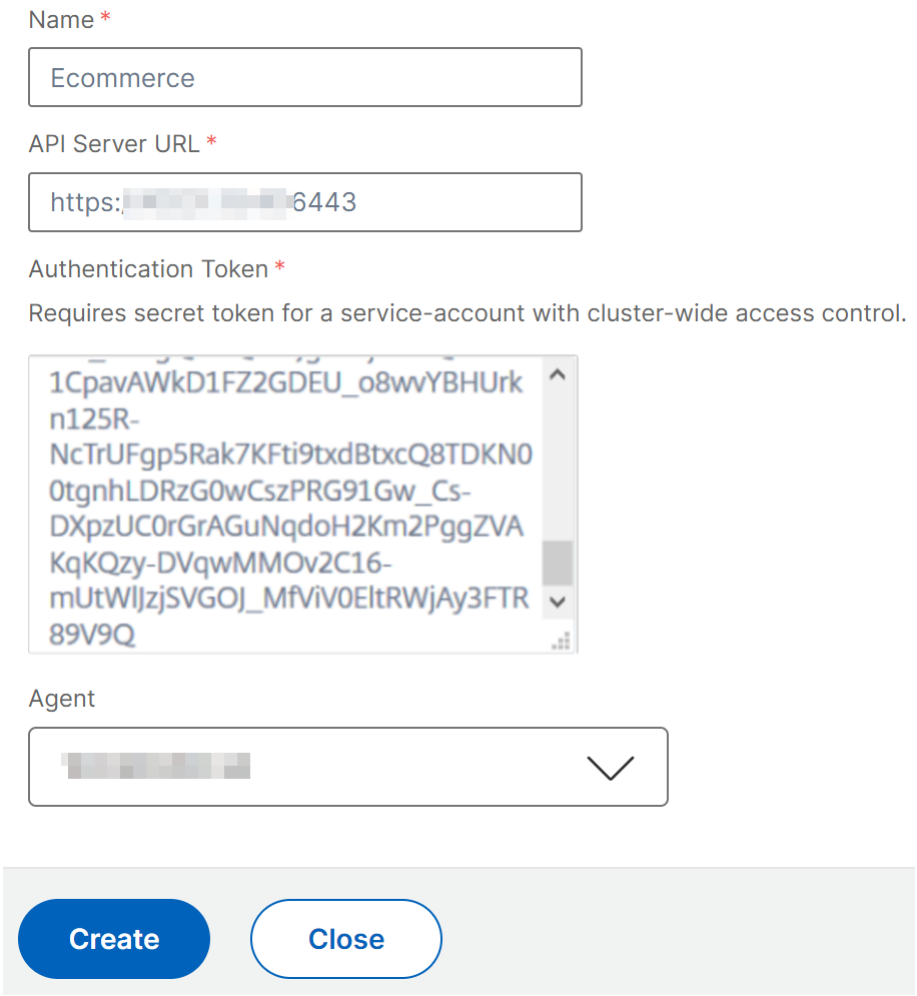

```
kubectl describe secret <token-name>
```

ii. 复制生成的令牌并将其粘贴为身份验证令牌

有关更多信息，请参阅 Kubernetes 文档。

d) 从列表中选择座席。

e) 单击创建。



灵活和池化许可的许可证管理

September 2, 2024

> 注意：
>
> 当您购买通用混合多云 (UHMC) 或 Citrix 平台许可 (CPL) 时，交付的 NetScaler 许可证被称为灵活许可证。

许可证文件

NetScaler 灵活许可证包括以下文件，您必须从 MyCitrix 门户网站下载这些文件。有关从当前类型的 NetScaler 许可过渡到灵活许可的更多信息，请参阅过渡到灵活许可。

本节列出了您的 NetScaler 上存在的许可文件。

文件名包含	说明	下载信息	在哪里上载/申请许可证
NetScaler Flexed VPX SW 实例	使您有权使用 VPX/CPX/BLX 软件实例	使用您的 NetScaler 控制台主机 ID 下载此文件	在 NetScaler 控制台上
NetScaler Flexed MPX SW 实例	使您有权使用 MPX 软件实例	使用您的 NetScaler 控制台主机 ID 下载此文件	在 NetScaler 控制台上
NetScaler Flexed SDX SW 实例	使您有权使用 SDX 软件实例	使用您的 NetScaler 控制台主机 ID 下载此文件	在 NetScaler 控制台上
NetScaler Flexed Platinum BW	使您有权获得 Flexed Platinum 吞吐容量	使用您的 NetScaler 控制台主机 ID 下载此文件	在 NetScaler 控制台上
NetScaler Flexed VPX FIPS SW 实例	使您有权使用 VPX FIPS 软件实例	使用您的 NetScaler 控制台主机 ID 下载此文件	在 NetScaler 控制台上
零容量 MPX-Z 平台许可证	使您有权让 NetScaler MPX HW 参与灵活许可	下载此文件	在 NetScaler MPX 上
零容量 SDX-Z 平台许可证	使您有权让 NetScaler SDX HW 参与灵活许可	下载此文件	在 NetScaler SDX 上

需要注意的重要事项

1. 如果您是过渡到灵活许可的池化许可客户，并且您的 MPX 和 SDX 硬件已经拥有 Z-Cap 永久许可证，则无需申请通过灵活获得的 Z-Cap 许可证。但是，如果在 NetScaler MPX/NetScaler SDX 上申请的当前 Z-Cap 许可在特定期限内有效，则必须申请与灵活许可一起获得的 Z-Cap 许可。灵活软件许可证包括 NetScaler Flexed MPX/SDX/VPX/VPX FIPS 软件实例和 NetScaler Flexed Platinum 带宽许可证。
2. 您必须在 NetScaler 控制台上为部署中使用的 NetScaler 外形规格申请灵活许可证。例如：

   如果您使用的是 NetScaler SDX 外形规格，请应用以下许可：

许可证文件	适用对象
NetScaler Flexed SDX SW 实例	NetScaler 控制台
NetScaler Flexed VPX SW 实例	NetScaler 控制台
NetScaler Flexed Platinum BW	NetScaler 控制台
ADC 零容量 SDX-Z 平台	NetScaler SDX

如果您使用的是 NetScaler MPX 外形规格，请应用以下许可：

许可证文件	适用对象
NetScaler Flexed MPX SW 实例	NetScaler 控制台
NetScaler Flexed Platinum BW	NetScaler 控制台
ADC 零容量 MPX-Z 平台	NetScaler MPX

如果您使用的是 NetScaler VPX、NetScaler BLX 或 NetScaler CPX 外形规格，请申请以下许可：

许可证文件	适用对象
NetScaler Flexed VPX SW 实例	NetScaler 控制台
NetScaler Flexed Platinum BW	NetScaler 控制台

如果您使用的是 NetScaler VPX FIPS 外形规格，请应用以下许可

许可证文件	适用对象
NetScaler Flexed VPX FIPS SW 实例	NetScaler 控制台
NetScaler Flexed Platinum BW	NetScaler 控制台

申请许可证文件

您可以添加、删除和下载许可证。必须先申请许可证，然后才能使用。

1. 导航到 **NetScaler** 许可 **>** 许可管理。
2. 在“许可证文件”部分中，单击“添加许可证文件”，然后选择以下选项之一：
   - 从本地电脑上载许可文件：如果本地电脑上已经存在许可文件，则可以将其上载到 NetScaler 控制台。

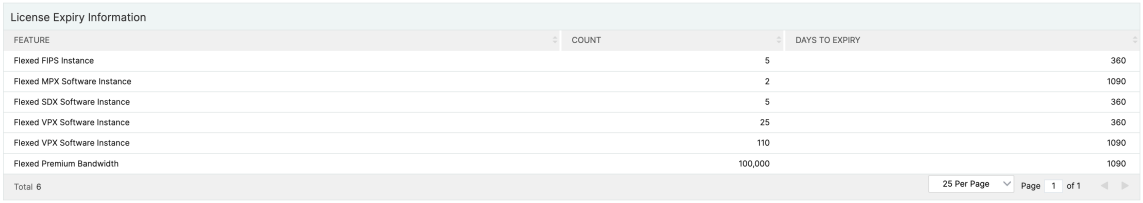
- 使用许可访问代码：为您从 Citrix 购买的许可指定许可访问代码。单击“获取许可证”，然后单击“完成”。

3. 单击完成。

   许可文件将添加到 NetScaler 控制台中。

   许可到期信息 部分列出了 NetScaler 控制台中存在的许可、数量以及剩余的到期天数。

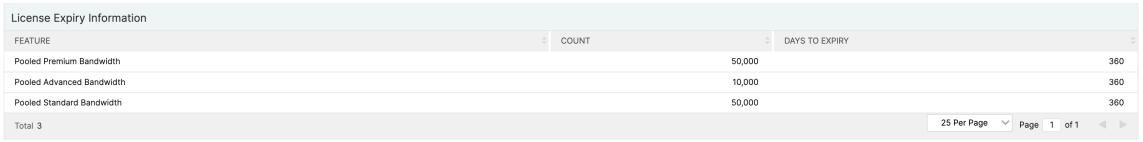
   以下屏幕截图显示了灵活的 NetScaler VPX、NetScaler MPX、NetScaler SDX 和 NetScaler VPX FIPS 软件实例许可的数量、现有的弹性高级带宽容量以及到期天数。

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Flexed FIPS Instance	5	360
Flexed MPX Software Instance	2	1090
Flexed SDX Software Instance	5	360
Flexed VPX Software Instance	25	360
Flexed VPX Software Instance	110	1090
Flexed Premium Bandwidth	100,000	1090

   Total 6 — 25 Per Page — Page 1 of 1

   以下屏幕截图显示了可用的标准池、高级带宽和高级带宽以及到期天数。

   
   License Expiry Information

FEATURE	COUNT	DAYS TO EXPIRY
Pooled Premium Bandwidth	50,000	360
Pooled Advanced Bandwidth	10,000	360
Pooled Standard Bandwidth	50,000	360

   Total 3 — 25 Per Page — Page 1 of 1

4. 选择许可证文件，然后单击“应用许可证”。

删除许可证文件

要删除许可证文件，请选择一个或多个文件，然后单击“删除”。删除许可证时，必须先添加许可证，然后才能应用该许可证。

下载许可证文件

要下载许可证文件，请选择一个文件并单击“下载”。您可以将许可证文件脱机保存为备份。

许可证服务器端口设置

NetScaler 实例使用端口与许可服务器通信。单击“编辑”图标并为以下参数指定值：

- 许可服务器端口：NetScaler 实例用于访问 Citrix 许可门户进行许可分配的代理服务器端口。默认值：27000。
- 供应商守护程序端口：NetScaler 实例用于与许可服务器通信的许可服务器端口。默认值：7279。

许可证到期信息

现在，您可以为灵活/合并容量许可证配置许可证的许可证到期阈值。设置阈值后，当许可到期时，NetScaler 控制台会通过电子邮件发送通知。当许可在 NetScaler 控制台上过期时，还会发送 SNMP 陷阱和通知。

发送许可到期通知时会生成一个事件，可以在 NetScaler 控制台上通过基础架构 **>** 事件查看该事件。

查看许可证到期时间

1. 导航到 **NetScaler** 许可 **>** 许可管理。
2. 在“许可证设置”页面的“许可证到期信息”部分下，您可以找到即将到期的许可证的详细信息：
    - 功能：即将到期的许可证类型。
    - 数量：将受到影响的虚拟服务器或实例的数量。
    - 到期天数：许可证到期前的天数。

> 注意：
>
> 当您向池中添加新许可时，NetScaler 实例将在其现有许可到期时使用新许可。

通知设置

指定根据哪些设置发送有关许可证分配和到期天数的通知。

1. 在“通知设置”部分，单击“编辑”图标，然后选择“许可证使用时通知我”。将警报阈值设置为分配给发送通知的灵活/池化许可证容量的百分比。
2. 选中相应的复选框，选择要在许可证达到阈值或即将到期时发送的通知类型。通知类型如下。
    - 电子邮件：用于发送通知的电子邮件配置文件或分发列表。有关更多信息，请参阅创建电子邮件分发列表。
    - **Slack**：用于发送通知的 Slack 配置文件详情。
    - **PagerDuty**：用于发送通知的 PagerDuty 配置文件。
    - **ServiceNow：Citrix ServiceNow 配置文件是默认指定的，是目前唯一可用的选项。
      有关创建这些配置文件的更多信息，请参阅 配置通知

    Select a notification type and click **Add** to add details. You can also test each notification system before saving your settings.
3. 指定到期天数，即您希望在许可证到期前收到许可证到期通知的天数。
4. 单击保存。

创建电子邮件通讯组列表

执行以下步骤创建电子邮件通讯组列表：

1. 选择“电子邮件”，然后单击“添加”。
2. 在 创建电子邮件通讯组列表中，指定以下详细信息：
    - 名称 -指定通讯组列表名称。

- 电子邮件服务器 - 选择发送电子邮件通知的电子邮件服务器。要添加电子邮件服务器，请单击“添加”。指定服务器名称/IP 地址和端口。选择“身份验证”以强制进行身份验证才能访问电子邮件服务器。如果电子邮件服务器支持 SSL 身份验证，请选择安全。单击创建。
- 发件人 - 指定 NetScaler 控制台发送消息的电子邮件地址。
- 收件人 - 指定 NetScaler 控制台向其发送消息的电子邮件地址。
- 抄送 -指定 NetScaler 控制台将消息复制到的电子邮件地址。
- 密件抄送 -指定 NetScaler 控制台隐蔽抄送邮件（不显示邮箱地址）的邮箱地址。

3. 单击创建。

创建 **Slack** 配置文件

执行以下步骤来创建“Slack”配置文件：

1. 在“**Slack**”中，单击“添加”。
2. 在 创建 **Slack** 配置文件中，指定以下详细信息：

   - 配置文件名称 -指定配置文件名称。此名称显示在 Slack 配置文件列表中。
   - 通道名称 -指定 NetScaler 控制台向其发送通知的 Slack 通道名称。
   - **Webhook URL** -指定该频道的 Webhook URL。传入的 Webhook 是将来自外部来源的消息发布到 Slack 的简单方法。URL 在内部链接到频道名称。发送到此 URL 的所有事件通知都发布在指定的 Slack 通道上。网络挂钩的示例如下：https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK。

创建 **PagerDuty** 配置文件

PagerDuty 使您能够通过电子邮件、推送通知和注册号码上的电话来配置通知。在 NetScaler 控制台中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。要开始使用 PagerDuty，请参阅 PagerDuty 文档。

请执行以下步骤来创建 PagerDuty 配置文件：

1. 在“**PagerDuty**”中，单击“添加”。
2. 在 创建 **PagerDuty** 配置文件中，指定以下详细信息：

   - 配置文件名称 -指定配置文件名称。不同的模块（例如事件规则和 SSL 通知）使用此名称来发送 PagerDuty 警报。
   - 集成密钥 -指定集成密钥。您可以从您的 PagerDuty 门户网站获取此密钥。

3. 单击创建。

有关更多信息，请参阅 PagerDuty 文档中的 服务和集成 。

查看 **ServiceNow** 配置文件

要启用 NetScaler 事件的 ServiceNow 通知，必须使用 ITSM 连接器将 NetScaler 控制台与 ServiceNow 集成在一起。有关更多信息，请参见 将 NetScaler 控制台与 ServiceNow 实例集成。

执行以下步骤以查看和验证 ServiceNow 配置文件：

1. 在 **ServiceNow** 中，默认选择 **Citrix_Workspace_SN** 配置文件。
2. 单击“测试”自动生成 ServiceNow 票证并验证配置。

> 注意：
>
> 有关不同类型的 NetScaler 许可的信息，请参见许可概述。

灵活和池化许可的最小和最大容量

April 10, 2024

NetScaler 灵活许可使用配置为许可服务器的 NetScaler 控制台来管理灵活许可：带宽池许可和实例池许可。

从带宽和实例池中签出许可时，零容量硬件上的 NetScaler 外形规格和硬件型号决定：

- NetScaler 实例在正常运行之前必须签出的最小带宽和实例数。
- NetScaler 可以签出的最大带宽和实例数。
- 每次带宽检查的最小带宽单位。最小带宽单位是 NetScaler 必须从池中检出的最小带宽单位。任何签出都必须是最低带宽单位的整数倍数。例如，如果 NetScaler 的最小带宽单位为 1 Gbps，则可以检出 1000 Gbps，但不能检出 200 Mbps 或 150.5 Gbps。最小带宽单位不同于最低带宽要求。NetScaler 实例只有在获得至少最小带宽许可后才能运行。一旦满足最低带宽，实例就可以以最低带宽单位的倍数来查看更多带宽。

表 1 至表 5 汇总了所有支持的 NetScaler 实例的最大带宽/实例、最小带宽/实例和最低带宽单位。表 6 汇总了所有支持的 NetScaler 实例对不同外形规格的许可要求。下表涉及系统要求。

> 注意：
>
> NetScaler CPX/BLX/VPX 的最低带宽结账单位为 10 Mbps。NetScaler MPX/SDX 的最低带宽结账单位为 1 Gbps。

表 **1.** 支持 **MPX** 的弹性容量

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最低带宽单位
MPX 5900Z	1	10	1 Gbps
MPX 8900Z	5	30	1 Gbps
MPX 8900Z FIPS	5	20	1 Gbps
MPX 9100Z	10	95	1 Gbps
MPX 9100Z FIPS	10	95	1 Gbps
MPX 14000Z	20	100	1 Gbps
MPX 14000Z-40G	20	100	1 Gbps
MPX 14000Z-40S	40	100	1 Gbps
MPX 14000Z FIPS	30	80	1 Gbps
MPX 15000Z	20	120	1 Gbps
MPX 15000Z-50G	20	120	1 Gbps
MPX 15000Z FIPS	30	120	1 Gbps
MPX 16000Z	30	250	1 Gbps
MPX 22000Z	40	120	1 Gbps
MPX 24000Z	100	150	1 Gbps
MPX 25000Z	100	160	1 Gbps
MPX 25000Z-40G	100	200	1 Gbps
MPX 26000Z	100	200	1 Gbps
MPX 26000Z-50S	100	200	1 Gbps
MPX 26000Z-100G	100	200	1 Gbps

表 **2A.** 支持版本早于 **13.0-47.x** 的 **NetScaler SDX** 版本的弹性容量

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX 8900Z	10	30	2	7	1 Gbps
SDX 14000Z	20	100	5	25	1 Gbps
SDX 14000Z-40G	40	100	20	25	1 Gbps

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX 15000Z	20	120	5	55	1 Gbps
SDX 15000Z-50G	20	120	5	55	1 Gbps
SDX 22000Z	40	120	80	80	1 Gbps
SDX 24000Z	100	150	80	80	1 Gbps
SDX 25000Z	100	200	20	115	1 Gbps
SDX 25000Z-40G	100	200	20	115	1 Gbps
SDX 26000Z	100	200	20	115	1 Gbps
SDX 26000Z-50S	100	200	20	115	1 Gbps
SDX 26000Z-100G	100	200	20	115	1 Gbps

表 **2B.** 支持 **NetScaler SDX** 版本 **13**（版本 **13.0-47.x** 及更高版本）、版本 **13.1**（版本早于 **51.x**）和 **14.1** 版（版本 **12.x** 之前的版本）的弹性容量

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	2	7	1 Gbps
SDX 14000Z	10	100	2	25	1 Gbps
SDX 14000Z-40G	20	100	10	25	1 Gbps
SDX 15000Z	10	120	2	55	1 Gbps
SDX 15000Z-50G	10	120	2	55	1 Gbps
SDX 16000Z	15	250	10	55	1 Gbps
SDX 22000Z	20	120	40	80	1 Gbps
SDX 24000Z	50	150	40	80	1 Gbps

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX 25000Z	50	200	10	115	1 Gbps
SDX 25000Z-40G	50	200	10	115	1 Gbps
SDX 26000Z	50	200	10	115	1 Gbps
SDX 26000Z-50S	50	200	10	115	1 Gbps
SDX 26000Z-100G	50	200	10	115	1 Gbps

表 **2C.** 支持 **NetScaler SDX** 版本 **13.1**（版本 **51.x** 及更高版本）和版本 **14.1**（版本 **12.x** 及更高版本）的弹性容量

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX 8900Z	5	30	1	7	1 Gbps
SDX 9100Z	10	95	1	7	1 Gbps
SDX 14000Z	10	100	1	25	1 Gbps
SDX 14000Z-40G	20	100	1	25	1 Gbps
SDX 15000Z	10	120	1	55	1 Gbps
SDX 15000Z-50G	10	120	1	55	1 Gbps
SDX 16000Z	15	250	1	55	1 Gbps
SDX 22000Z	20	120	1	80	1 Gbps
SDX 24000Z	50	150	1	80	1 Gbps
SDX 25000Z	50	200	1	115	1 Gbps
SDX 25000Z-40G	50	200	1	115	1 Gbps
SDX 26000Z	50	200	1	115	1 Gbps

产品系列	最小带宽 (Gbps)	最大带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX 26000Z-50S	50	200	1	115	1 Gbps
SDX 26000Z-100G	50	200	1	115	1 Gbps

> 备注：
>
> - 最低购买量可能与最低系统要求不同。
> - 在运行版本 14.1-12.x 及更高版本且拥有灵活许可的 NetScaler SDX 上，取消了签出最低实例许可数量的限制。也就是说，您可以签出至少一个实例许可证。

表 **3. NetScaler CPX** 实例支持的最小/最大带宽和最小/最大实例

产品系列	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例数	最大实例数	最低带宽单位
CPX	10	10	1	1	10 Mbps

表 **4.** 虚拟机管理程序和云服务上的 **NetScaler VPX** 实例支持的最小/最大带宽和最小/最大实例

虚拟机管理程序/云服务	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例数	最大实例数	最低带宽单位
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps
Google Cloud	10 Gbps	10 Mbps	1	1	10 Mbps

> 注意：
>
> 最小采购数量不同于最低系统要求。

表 **5. NetScaler BLX** 实例支持的最小/最大带宽和最小/最大实例

产品系列	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例数	最大实例数	最低带宽单位
BLX	100	10	1	1	10 Mbps

表 **6.** 不同外形规格的零容量许可证要求

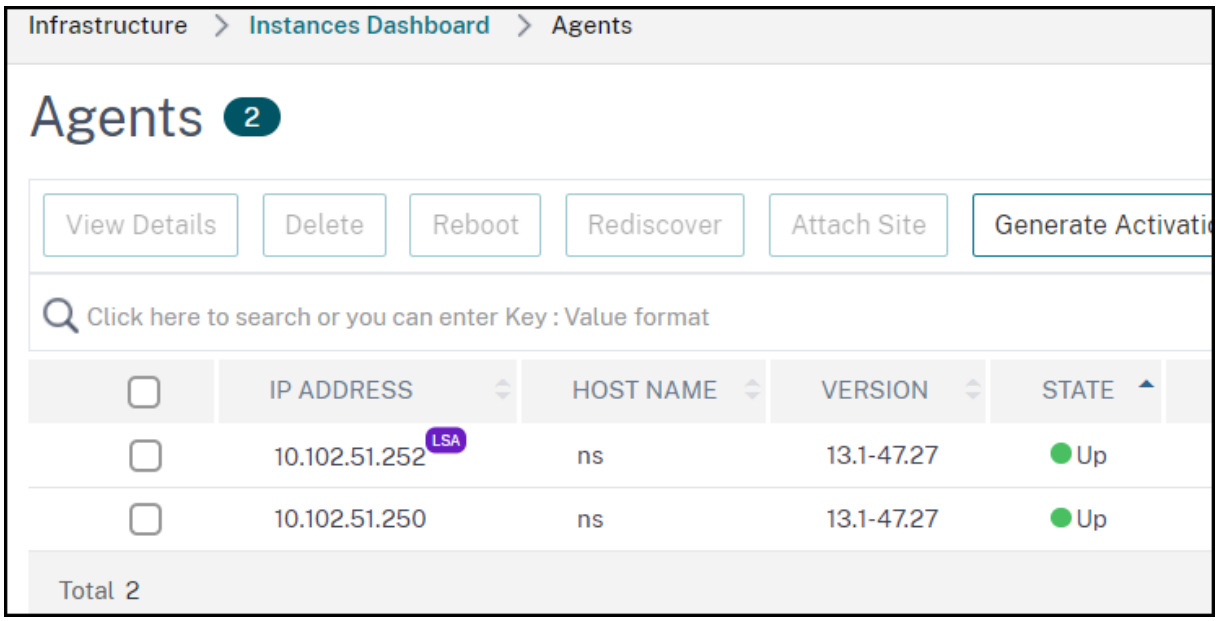
产品系列	零容量硬件
MPX	需要许可证
SDX	需要许可证
VPX	-
CPX	-
BLX	-

灵活或池化许可的 **NetScaler** 代理行为

April 10, 2024

NetScaler 代理充当 NetScaler 控制台与跨不同数据中心和公有云发现的实例之间的中介。NetScaler 控制台服务要求每个租户至少有一个代理才能使用灵活或池化许可。每个站点或多站点可以部署多个 NetScaler 代理，但在整个租户部署中，只有一个代理可以具有许可服务器代理 (LSA) 角色。

以下示例显示部署了两个代理，其中一个具有 LSA 角色：



LSA 是一种代理，可在基于 NetScaler 控制台服务的池化许可部署中用作许可服务器。如果 LSA 出现故障，该服务将等待 24 小时才能选出新的 LSA。

在此之前，使用池化或灵活许可的 NetScaler 实例处于宽限期。作为管理员，您也可以手动选择 LSA。

手动选择 **NetScaler** 控制台代理作为 **LSA**

管理员可以手动选择 NetScaler 控制台代理作为 NetScaler 池化许可或 NetScaler 灵活许可的 LSA。当 LSA 关闭时，NetScaler 控制台服务会等待 24 小时后才会自动选择下一个 LSA。在此期间，管理员可以使用此功能手动选择新的 LSA。但是，管理员必须确保当选的新 LSA 的状态为 UP 且其诊断状态为 OK。

当管理员手动选择新的 LSA 时，许可功能最多可能需要 5 分钟才能正常运行。在此期间，NetScaler 实例处于宽限期，任何新的许可签出都将失败。

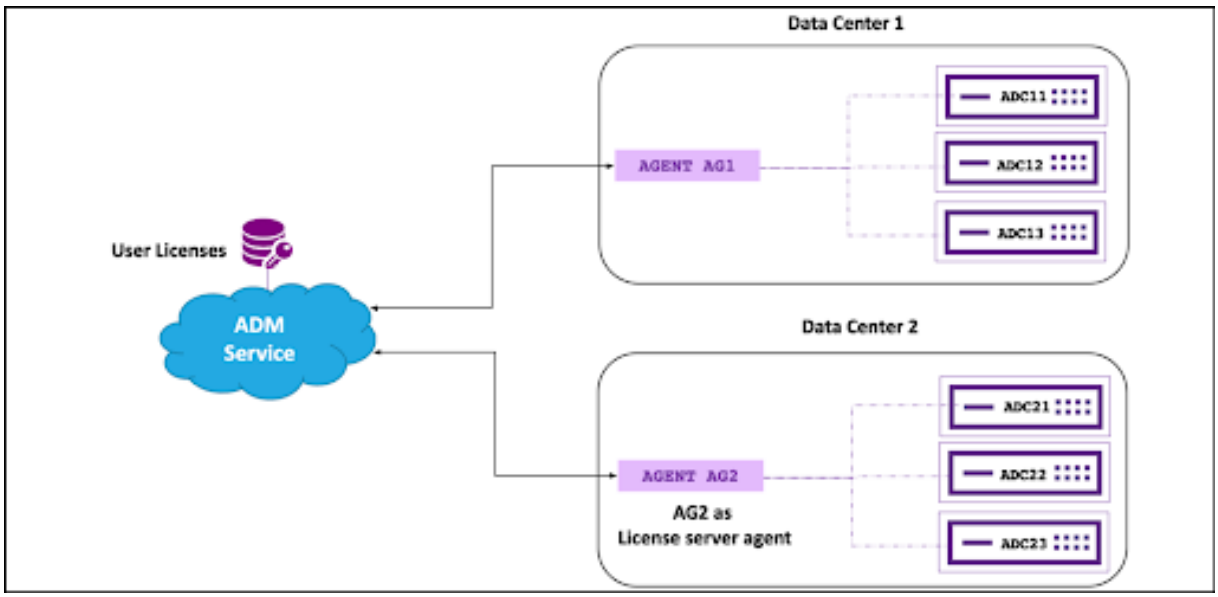
要选择 LSA，请执行以下操作：

1. 导航到基础架构 **>** 实例控制面板 **>** 代理，然后选择一个代理。
2. 在“选择操作”列表中，选择“设置为 **LSA**”。
3. 单击是进行确认。所选代理担任 LSA 角色。

多个 **NetScaler** 代理行为

在组合了多个代理和多个站点的部署中，NetScaler 代理遵循客户端/服务器架构。

在 UP 状态下注册的第一个/最早的代理被分配 LSA 角色。稍后添加的任何其他代理都将充当代理，并与托管主 LSA 角色的代理进行通信以进行许可证分配。托管代理角色的每个代理都通过 NetScaler 控制台服务与具有当前 LSA 角色的代理通信。



> 注意
>
> 担任 LSA 角色的代理与其他（非 LSA）代理之间没有直接通信。所有连接仅通过 NetScaler 控制台服务。

NetScaler 代理故障转移行为

代理故障转移在多代理部署中的工作方式如下。

假设在同一个数据中心中有两个代理，即 AG1 和 AG2。

- AG1 配置为使用 ADC11、ADC12、ADC13 作为远程许可证主机或 LSA。
- AG2 配置为使用 ADC21、ADC22、ADC23 作为远程许可证主机或 LSA。
- AG2 充当许可证服务器。
  - 如果 AG1 出现故障，ADC11、ADC12 和 ADC13 会自动通过 AG2 进行连接以协调许可证。
    - 在重新连接发生时，如果错过了几次心跳，ADC11、ADC12 和 ADC13 可能仍会注意到一小段宽限期。
  - 如果 AG2 出现故障，所有 ADC 将继续保持宽限状态，直到：
    - 要么将 AG2 恢复/重新启动，要么在 24 小时后由 NetScaler 控制台服务自动选择 AG1 作为新的 LSA，要么由管理员手动选择。
    - 或者 AG2 已从 NetScaler 控制台服务中删除。注销后，NetScaler 控制台服务会将 AG1 指定为具有 LSA 角色的代理。
    - 选举完成后，AG1 开始向配置的实例分配和协调资源。

有关 LSA 的问题，请参阅 许可证服务器代理上的常见问题解答。

灵活许可证

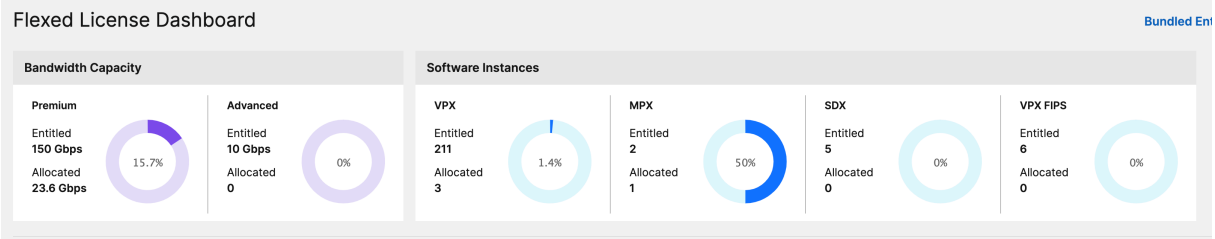
April 10, 2024

NetScaler 灵活许可是新的许可框架，旨在简化许可管理流程。您的灵活许可证包括软件实例许可证（VPX/CPX/BLX、SDX、MPX 和 VPX FIPS）和带宽容量许可证。您必须在 NetScaler 控制台服务或 NetScaler ADM 本地上申请灵活许可。您还必须分别在 NetScaler MPX 和 NetScaler SDX 硬件上申请 MPX Z-Cap 和 SDX Z-Cap 许可。然后，您可以将它们分配给部署在云端或本地的所有 NetScaler 外形规格。

Flexed 许可证还提供对无限虚拟服务器的分析。

如果您之前拥有池化许可证并购买了灵活许可证，则可以在灵活许可证控制面板中查看您的许可证详细信息。组合后的带宽和实例显示在灵活许可证控制板中。

除非您之前拥有标准池或高级许可证，否则带宽许可证通常仅包括高级版，在这种情况下，标准版、高级版和高级版会显示在灵活许可证控制面板中。



有关更多详细信息，请参阅灵活许可证控制面板。

您可以使用灵活许可确保为实例分配必要的带宽，但不超过其需求，从而最大限度地提高带宽利用率。在不影响流量的情况下，增加或减少在运行时分配给实例的带宽。

零容量硬件

当通过 NetScaler 灵活许可进行管理时，MPX 和 SDX 实例被称为“零容量硬件”，因为这些实例只有在将资源从带宽池中检出后才能运行。因此，这些平台也称为 MPX-Z 和 SDX-Z 装置。

零容量硬件需要 Z-cap 许可证才能查看公共池中的带宽。

> 注意：
>
> - 零容量许可证的安装与其他 NetScaler 本地许可证的工作方式相同。有关如何获取和安装零容量许可证的更多信息，请参阅 NetScaler 许可指南。

管理和安装 **Z-cap** 许可证

必须使用硬件序列号或许可证访问代码手动安装 Z-cap 许可证。安装 Z-cap 许可后，它将锁定到硬件，无法按需在 NetScaler 硬件实例之间共享。但是，您可以手动将 Z-cap 许可移至另一个 NetScaler 硬件实例。

运行 NetScaler 软件版本 11.1 版本 54.14 或更高版本的 NetScaler MPX 实例以及运行 11.1 版本 58.13 或更高版本的 NetScaler SDX 实例支持 NetScaler 灵活许可。有关更多信息，请参阅灵活和池化许可的最小和最大容量中的表 1 和 2。

独立 **NetScaler VPX** 实例

在以下虚拟机管理程序上运行 NetScaler 软件版本 11.1 Build 54.14 及更高版本的 NetScaler VPX 实例支持灵活许可：

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 12.0 Build 51.24 及更高版本的 NetScaler VPX 实例支持灵活许可：

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 13.0 和 13.1（所有版本）的 NetScaler VPX 实例支持灵活许可：

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

独立的 **NetScaler CPX** 实例

部署在 Docker 主机上的 NetScaler CPX 实例支持灵活许可。与零容量硬件不同，NetScaler CPX 不需要 Z-cap 许可。单个 NetScaler CPX 实例消耗高达 1 Gbps 的吞吐量，只能检出 1 个实例，没有来自许可池的带宽。例如，假设您有 20 个 NetScaler CPX 实例，带宽池为 20 Gbps。如果其中一个 NetScaler CPX 实例消耗 500 Mbps 的吞吐量，则其余 19 个 NetScaler CPX 实例的带宽池仍为 20 Gbps。

如果同一 NetScaler CPX 实例开始消耗 1500 Mbps 的吞吐量，则其余 19 个 NetScaler CPX 实例的带宽池将达到 19.5 Gbps。

对于灵活许可，只能以 10 Mbps 的倍数添加更多带宽。

独立 **NetScaler BLX** 实例

NetScaler BLX 实例支持灵活许可。NetScaler BLX 实例不需要 Z-cap 许可。要处理流量，NetScaler BLX 实例必须从池中签出带宽和实例许可证。

带宽池

带宽池是 NetScaler 实例（物理和虚拟）可共享的总带宽。带宽池包括高级软件版本的池。如果您从池化许可转为灵活许可，您可能会发现标准版、高级版和高级版软件的混合版本。给定的 NetScaler MPX/VPX/CPX/BLX 实例不能同时检出来自不同池的带宽。可从其签出带宽的带宽池取决于为其许可的软件版本。

实例池

软件实例池有三种类型：

- VPX/CPX/BLX 软件实例
- MPX 软件实例（同样的池适用于 MPX FIPS）
- SDX 软件实例（同样的池适用于 SDX FIPS）
- VPX FIPS 软件实例

从池中签出后，许可证会解锁软件实例的资源，包括 CPU/PE、SSL 内核、每秒数据包和带宽。

配置灵活许可

January 29, 2024

> 注意：
>
> 如果您拥有合并许可证，并且现在已经购买并应用了灵活许可证，则合并后的授权现在会显示在 Flexed 许可证控制面板中。

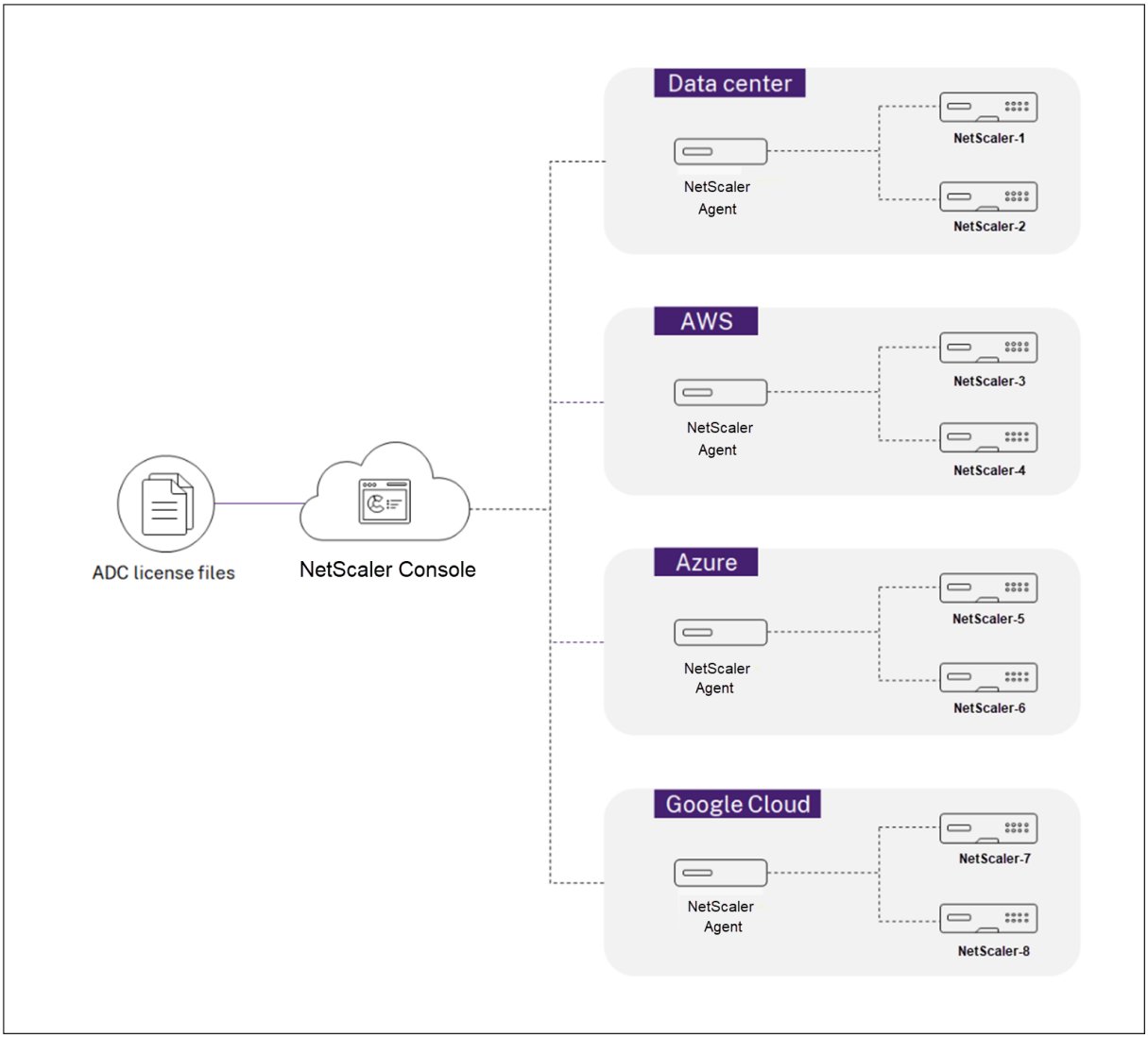
NetScaler 灵活许可允许您在不同的 NetScaler 外形规格之间共享带宽或实例许可。将此灵活容量用于数据中心或公有云中的实例。当实例不再需要资源时，它会将分配的容量重新检查到公用池中。在其他需要资源的 NetScaler 实例上重复使用已释放的容量。

您可以使用 Flexed 许可确保为实例分配必要的带宽，但不超过其需求，从而最大限度地提高带宽利用率。在不影响流量的情况下，增加或减少在运行时分配给实例的带宽。

要使用 NetScaler 灵活许可，必须将 NetScaler 控制台代理连接到 NetScaler 实例。NetScaler 实例通过代理从 NetScaler 控制台签入和签出许可。

您可以在 NetScaler 控制台中执行以下任务：

1. 将 Flexed 许可证文件（带宽池或软件实例池）上载到许可证服务器。
2. 将 SDX 或 MPX 零容量许可上载到 SDX 或 MPX 硬件，并根据需要将许可池中的许可分配给 NetScaler 实例。
    - 根据实例的最小和最大容量查看 NetScaler 实例的许可。



您可以从 citrix.com 下载灵活许可证，包括带宽、实例和 Z-cap 许可证。有关更多信息，请参阅 NetScaler 许可指南。

NetScaler 灵活的许可状态

灵活许可状态指示 NetScaler 实例的许可要求。使用灵活许可配置的 NetScaler 实例显示以下状态之一：

- 已分配：实例以适当的许可证容量运行。
- 宽限：实例正在使用宽限许可证运行。
- 连接丢失：从 NetScaler 控制台到实例的通信无法正常工作。

开始之前的准备工作

在配置 Flexed 许可之前，请确保满足以下先决条件：

- 在 NetScaler 控制台中安装和注册代理。要安装和注册代理，请参阅 入门。
- 确保所有注册代理都处于 UP 状态，以便 Flexed 许可正常运行。如果代理处于 DOWN 状态但尚未停用或终止，请将其置于 UP 状态。如果 DOWN 代理已停用、终止或不再使用，请将其从 NetScaler 控制台中删除。
- 27000和 7279端口可用于将许可从 NetScaler 控制台签出到实例。请参阅“系统要求”。

第 1 步-在 NetScaler 控制台中申请许可

1. 导航到 **NetScaler** 许可 **>** 许可管理。
2. 在“许可证文件”部分中，选择“添加许可证文件”，然后选择以下选项之一：
   - 从本地计算机上载许可证文件。如果您的本地电脑上已经存在许可文件，则可以将其上载到 NetScaler 控制台。
   - **Use license access code**（使用许可证访问代码）。为您从 Citrix 购买的许可证指定许可证访问代码。然后，选择 获取许可证。然后选择完成。

   > 注意：
   >
   > 您可以随时从“许可设置”向 NetScaler 控制台添加更多许可。

3. 单击完成。

   许可文件将添加到 NetScaler 控制台中。许可到期信息 部分列出了 NetScaler 控制台中存在的许可以及剩余的到期天数。

4. 在 许可证文件中，选择要应用的许可证文件，然后单击 应用许可证。

   此操作允许 NetScaler 实例将所选许可用作 Flexed 许可。

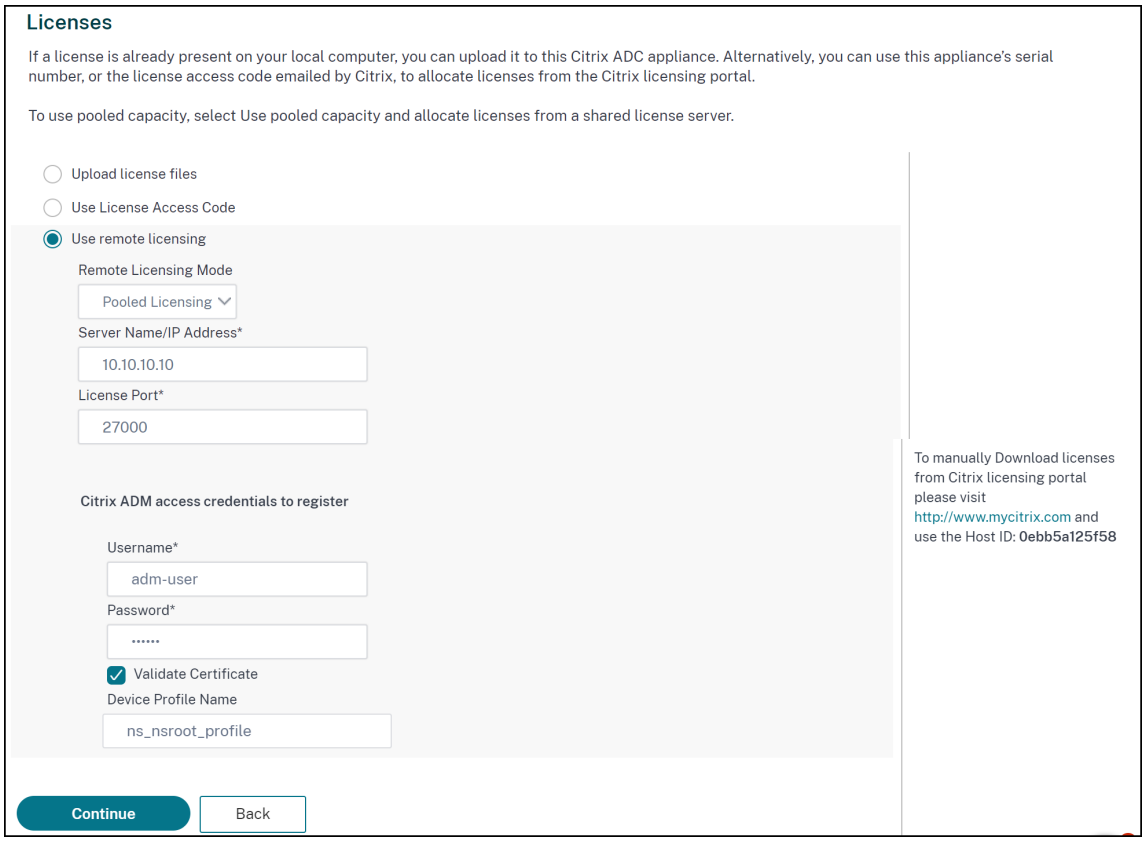
第 2 步-将 NetScaler 控制台注册为许可服务器并分配许可

您可以使用代理将 NetScaler 控制台注册为 NetScaler 实例的许可服务器。

使用 GUI 注册 NetScaler 控制台代理

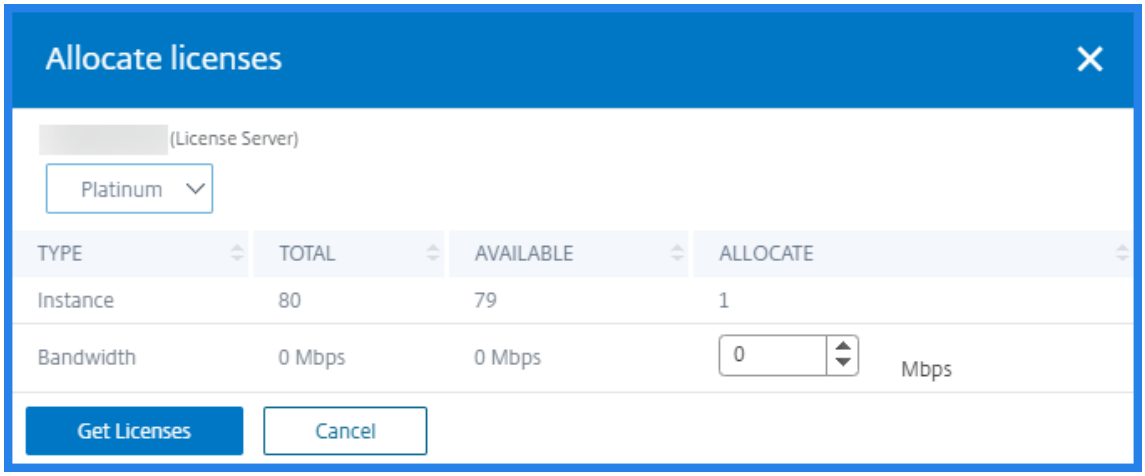
在 NetScaler 控制台 GUI 中，注册与 NetScaler 实例关联的 NetScaler 控制台代理。

1. 登录到 NetScaler GUI。
2. 导航到“系统”>“许可证”>“管理许可证”。
3. 单击“添加新许可证”。
4. 选择 使用远程许可，然后从列表中选择远程许可模式。
5. 在“服务器名称/IP 地址”字段中，指定在 NetScaler 控制台中注册的关联的 NetScaler 控制台代理的 IP 地址。
6. 选择“向 NetScaler 控制台注册”。
7. 输入您的 NetScaler 控制台代理凭据以在 NetScaler 控制台中注册实例，然后单击“继续”。在 NetScaler 控制台中，其中一个代理是许可服务器。



8. 在 分配许可证中，选择许可证版本并指定所需的带宽。

   首次在 NetScaler 中分配许可证。稍后您可以通过 NetScaler 控制台 GUI 更改或释放许可分配。



9. 单击 **Get Licenses**（获取许可证）。

> 重要
>
> 如果您更改了许可证版本，请热重启实例。在您重新启动实例之前，配置更改才会生效。

使用 **CLI** 添加 **NetScaler** 控制台代理

如果 NetScaler 实例没有 GUI，请使用以下 CLI 命令添加与实例关联的 NetScaler 控制台代理：

1. 登录 NetScaler 控制台。
2. 添加在 NetScaler 控制台中注册的关联的 NetScaler 控制台代理的 IP 地址：

```
1 > add ns licenseserver <adm-agent-IP-address> -port <adm-agent-
    license-port-number>
```

3. 查看许可证服务器中可用的许可证带宽：

```
1 > sh ns licenseserverpool
```

4. 从所需的许可证版本中分配许可证带宽：

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
```

> 重要信息：如果您更改许可证版本，则“
>
> 热”重新启动实例。
>
> ```
> reboot -w
> ```
>
> 在您重新启动实例之前，配置更改才会生效。

第 **3** 步**-**编辑 **NetScaler** 实例的弹性带宽

1. 导航到 **NetScaler** 许可 **>** 灵活许可 **>** 控制面板。
2. 在 许可的 **NetScalers** 部分中，选择一个实例，然后单击 编辑带宽。
3. 在“编辑带宽”页面中，在“分配”列中输入一个数字。
4. 单击 **Submit**（提交）。

NetScaler MPX-Z

MPX-Z 是支持灵活容量的 NetScaler MPX 设备。MPX-Z 仅支持高级版许可证的带宽池。

MPX-Z 需要许可证才能连接到许可证服务器。您可以使用以下方法之一安装 MPX-Z 许可证：

- 从本地计算机上载许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的“系统”>“许可证”部分中的许可证访问代码。

如果您移除 MPX-Z 许可证，MPX 将变为未获得许可。实例许可证将释放到许可证服务器。

您可以在不重新启动的情况下动态修改 MPX-Z 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重启实例时，它会自动签出其配置容量所需的灵活许可证。

NetScaler SDX-Z

SDX-Z 是支持灵活容量的 NetScaler SDX 设备。SDX-Z 支持高级版许可证的带宽和实例池。

SDX-Z 需要许可证才能连接到许可证服务器。您可以使用以下方法之一安装 SDX-Z 许可证：

- 从本地计算机上载许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的“系统”>“许可证”部分中的许可证访问代码。

如果您移除 SDX-Z 许可证，SDX 将变为未获得许可。实例许可证将释放到许可证服务器。

您可以在不重启的情况下动态修改 SDX-Z 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重启实例时，它会自动签出其配置容量所需的灵活许可证。

NetScaler 高可用性对

在开始之前，请确保将 NetScaler 控制台服务器配置为许可服务器。有关详细信息，请参见 将 NetScaler 控制台配置为许可服务器

当您为 NetScaler HA 对分配带宽时，NetScaler 控制台会检查分配给主实例的带宽。您必须对辅助实例重复该过程。

要向 NetScaler HA 对分配池许可，请参见向 NetScaler 实例分配灵活许可

弹性容量 页面分别显示实例及其分配的容量。

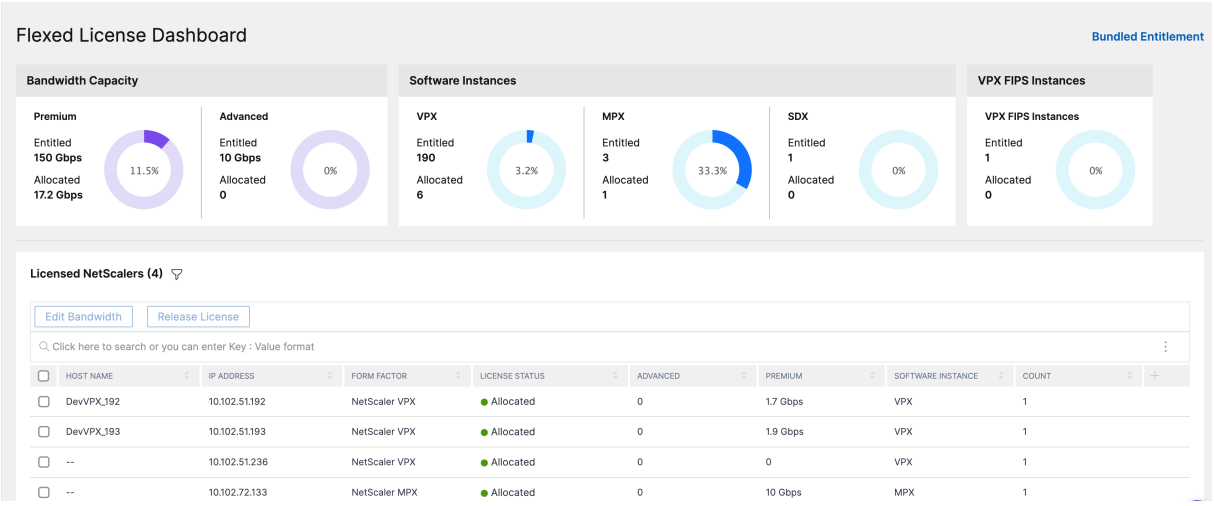
灵活许可证控制板

April 10, 2024

> 注意：
>
> 如果您之前有池化许可证，现在购买并应用了灵活许可证，则合并后的授权现在会显示在灵活许可证控制面板中。

灵活许可证控制板使您可以全面了解您购买的带宽容量和实例。

此页面上显示了各版本的带宽容量以及不同外形规格（例如 MPX、VPX 和 SDX）的实例详细信息。MPX 和 MPX FIPS 具有相同的许可证文件。同样，SDX 和 SDX FIPS 具有相同的许可证文件。但是，VPX FIPS 的文件与 VPX 不同，并且是单独显示的。此外，VPX（包括 SDX 上的 VPX）、BLX 和 CPX 需要 VPX 许可证，并且是 VPX 授权和分配的一部分。灵活的许可证仅支持高级版。但是，如果您购买了灵活许可证，并且之前已合并了标准或高级带宽容量，则与带宽容量（标准或高级）相关的详细信息也会列在灵活许可证控制面板中。



VPX（包括 SDX 上的 VPX）、BLX 和 CPX 规格要求使用 NetScaler Flexed VPX SW 实例许可证文件。也就是说，这些外形规格是 Flexed VPX SW 实例许可证的授权和分配的一部分。

有关您的许可的 NetScaler 实例的详细信息，请参阅“许可的 **NetScaler**”部分。您可以选择一个实例并编辑带宽或释放该实例的许可证。

您可以根据以下参数筛选结果：

- 按带宽过滤
  - Premium
  - 高级
  - Standard
- 外形规格
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
- 许可证状态
  - 连接已断开
  - 格蕾丝
  - 已分配

编辑 **NetScaler** 实例上分配的带宽

1. 导航到 **NetScaler** 许可 **>** 灵活许可 **>** 控制板。
2. 在 许可的 **NetScalers** 部分中，选择一个实例，然后单击 编辑带宽。
3. 在“编辑带宽”页面中，在“分配”列中输入一个数字。
4. 单击 **Submit**（提交）。

在 **NetScaler** 实例上发放许可

要将许可证转移到另一个实例，您必须释放当前实例的许可证，然后将许可证应用于新实例。选择“发布许可证”执行以下操作：

- 将在该实例上签出的所有许可证发放到许可证服务器。
- 删除该实例上的许可证服务器配置。

如果选择“是”，则您的 NetScaler 实例将变为未经许可且无法处理任何流量。

灵活许可证报告

June 7, 2024

在此控制板中，您可以查看有关以下内容的详细信息：

- 软件实例（VPX、MPX 和 SDX 以及 VPX FIP）授权和分配
- 带宽/吞吐量 - 容量授权、分配和实际使用量
- 所有托管或选定实例的峰值和平均分配
- 所有托管或选定实例的峰值和平均使用量

功能（适用于 NetScaler 实例）	说明
授权	软件实例类型（VPX、SDX、MPX）的总实例授权。
分配	软件实例类型（VPX、SDX、MPX）的总实例分配。

功能（用于带宽/吞吐量）	说明
授权	所有托管 NetScaler 实例的总带宽/吞吐量容量授权。总授权是根据许可管理（**NetScaler** 许可 **>** 许可证管理）中应用的许可证计算得出的。
分配	在灵活许可证控制板（**NetScaler** 许可 **>** 灵活许可 **>** 灵活许可证控制板）中分配给许可的 **NetScaler** 的带宽/吞吐量容量。
使用情况	NetScaler 实例消耗的总吞吐量。

> 注意：
>
> 灵活的许可证仅支持高级版。但是，如果您购买并申请了灵活许可证，并且之前已合并了标准或高级带宽容量，则还会列出与带宽/吞吐容量（标准或高级）相关的详细信息。例如，您已经申请了 1000 Gbps 灵活许可证（高级版），并且还拥有 100 Gbps 高级带宽的有效池化许可证，则报告控制板会显示高级 1000 Gbps 和 100 高级带宽。

以下示例可帮助您了解控制板如何显示峰值使用量和平均使用量：

假设有 3 个托管的 NetScaler 实例（NetScaler A、NetScaler B 和 NetScaler C）使用灵活许可（高级带宽），所选时长为 1 天。在计算时，NetScaler 控制台会考虑每个 NetScaler 实例每小时的数据点（以 Mbps 为单位）。在 1 天内，每个 NetScaler 实例有 24 个数据点。因此，对于 3 个 NetScaler 实例，有 (24 * 3) 个数据点。

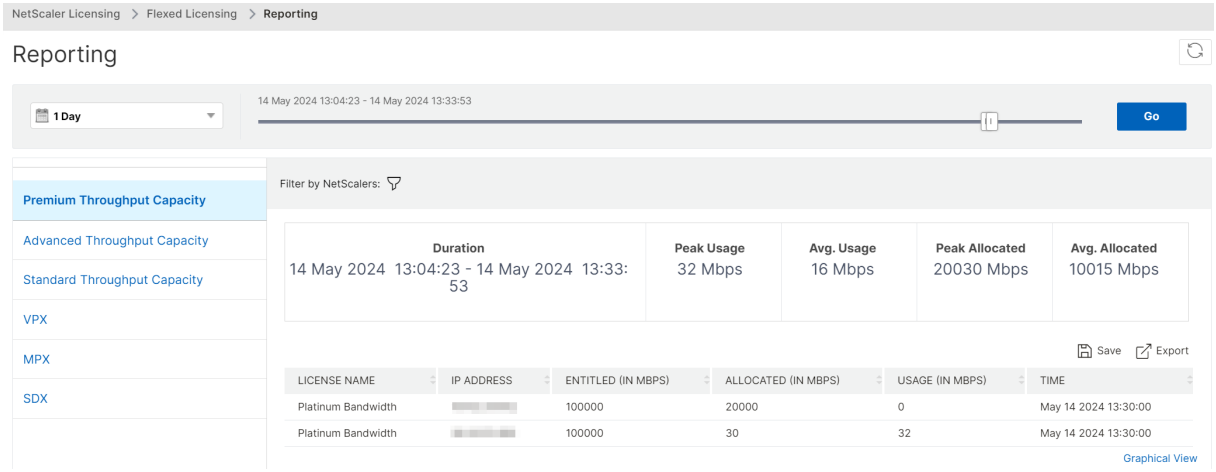
- 峰值使用量 = 所有 NetScaler 实例在 24 小时内最高数据点 (Mbps) 的总和。例如，如果 NetScaler A 的 24 小时内的最大数据点为 30 Mbps，NetScaler B 为 45 Mbps，NetScaler C 为 120 Mbps，则峰值使用量显示为 195 Mbps（30 + 45 + 120）。

- 平均使用量 = 每个 NetScaler 实例的所有 24 小时数据点之和除以 24。因此，对于 3 个 NetScaler 实例，所有 3 个 NetScaler 实例的总平均值除以 3。例如，如果 NetScaler A 的平均值为 25 Mbps，NetScaler B 的平均值为 20 Mbps，NetScaler C 的平均值为 45 Mbps，则平均使用量显示为 30 Mbps（25 + 20 + 35 除以 3）。

同样，峰值和平均分配详细信息使用相同的逻辑显示。

您可以从列表中选择持续时间，从一小时到一年，并以表格视图和图形视图查看详细信息。

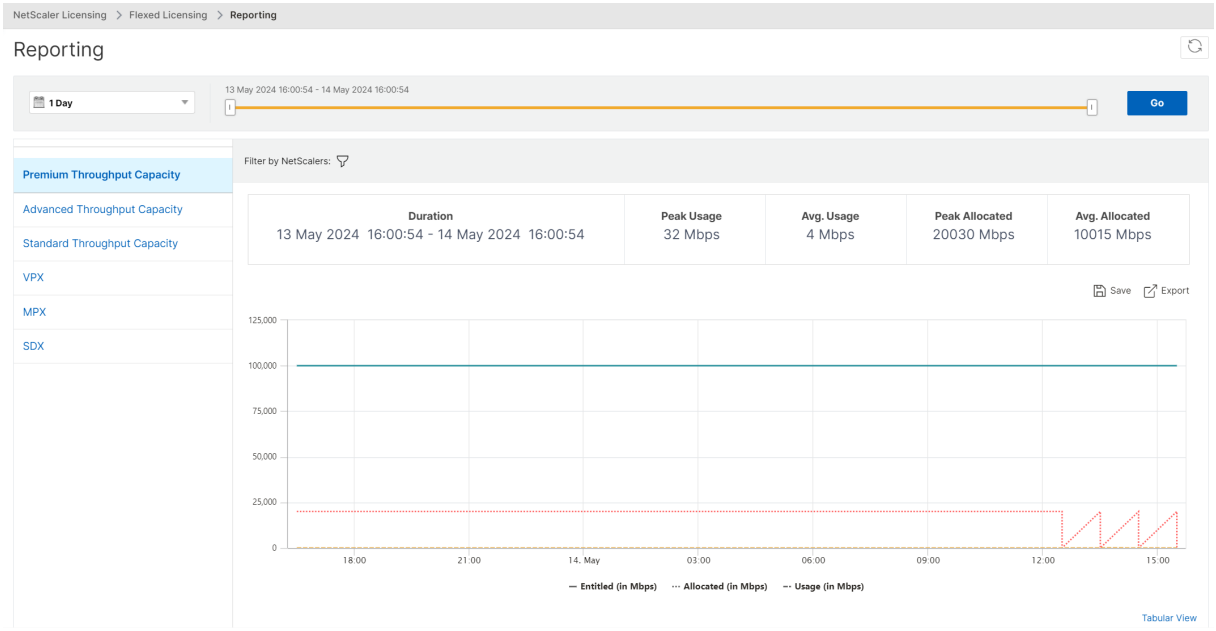
以下示例显示了使用灵活许可证（高级带宽）的实例的表格视图：



控制板上显示以下详细信息：

- 峰值使用量 - 选定时长内的最高使用量（以 Mbps 为单位）。
- 平均使用量 - 所选时长内的平均使用量（以 Mbps 为单位）。
- 分配的峰值 - 所选时段内的最高分配。
- 平均分配 - 所选时段内的平均分配。
- 筛选 - 您可以选择一个或多个实例来查看特定实例的使用情况和分配详细信息。
- 导出 - 您可以以 PDF、JPEG 和 PNG 格式导出详细信息。

以下示例显示了使用灵活许可证（高级带宽）的实例的图形视图：



过渡到灵活许可

April 10, 2024

> 注意：
>
> 您必须在当前许可证到期之前切换到灵活许可。在规划过渡时，请记住以下步骤，如果这些步骤涉及许可重新配置或 NetScaler 重启，请计划维护窗口。

将池带宽许可证改为灵活许可

有些步骤在 MPX、SDX 和 VPX 中很常见。首先列出这些步骤，然后是特定于 MPX、SDX 或 VPX 的步骤。

VPX/MPX/SDX 的常见步骤

1. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
2. 如果您拥有在特定时期内有效的 Z-Cap 软件许可证，请在 NetScaler 硬件 (MPX/SDX) 上申请该许可证。

适用于 **VPX/MPX**

需要执行下面额外的步骤：

1. 如果您拥有池化 Premium (Platinum) 带宽许可证，则该许可证将在旧许可证到期后自动切换到灵活。

2. 如果您拥有标准池化或高级池化带宽许可，请手动查看高级带宽并热重启 NetScaler。

适用于 **SDX**

> 注意：
>
> 确保在当前许可证到期之前切换到灵活许可。

需要执行下面额外的步骤：

1. 查看从灵活许可到 SDX 所需的实例和带宽许可证。不需要重新启动 SDX。
2. 如果 SDX 上的所有 VPX 都有 Premium 版本，则在旧许可证到期后，许可证会自动切换到灵活。
3. 将所有 VPX（在 SDX 上）的标准版或高级版更改为高级版。这些 VPX 实例会自动重启。
4. 将 SDX 的标准和高级带宽容量减少到零。

将 **vCPU** 池化为灵活许可

适用于 **VPX**

1. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
2. 使用 NetScaler GUI 删除现有许可证服务器。在所有步骤完成之前，NetScaler 是未经许可的。
3. 使用灵活/池化选项添加许可证服务器。
4. 查看 NetScaler 所需的实例和带宽许可证。
5. 热重启 NetScaler。

灵活许可的固定订阅或永久许可证

有些步骤在 MPX、SDX 和 VPX 中很常见。首先列出这些步骤，然后是特定于 MPX、SDX 或 VPX 的步骤。

VPX/MPX/SDX 的常见步骤

1. 载入 NetScaler 控制台。
2. 部署 NetScaler 代理。
3. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
4. 在 NetScaler 硬件 (MPX/SDX) 上申请 Z-Cap 软件许可。

适用于 **VPX/MPX**

需要执行下面额外的步骤：

1. 查看 NetScaler 所需的实例和带宽许可证。

2. 热重启 NetScaler。
3. 在 NetScaler 重新启动后，删除固定订阅许可证。

适用于 **SDX**

需要执行下面额外的步骤：

1. 查看 SDX 上的灵活许可中所需的实例和带宽许可证。
2. 如果 SDX 上的所有 VPX 都有高级版，则不需要重启 SDX。
3. 如果任何 VPX 具有高级版或标准版，则必须将该 VPX 转移到高级版。VPX 会自动重启。
4. 在 NetScaler SDX 上申请 Z-Cap 软件许可。
5. 查看 SDX 上的灵活许可中所需的实例和带宽许可证。
6. 在 NetScaler 重新启动后，删除固定订阅许可证。

将 **vCPU** 修复为灵活许可

适用于 **VPX**

1. 载入 NetScaler 控制台。
2. 部署 NetScaler 代理。
3. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
4. 在 NetScaler 上以灵活/池化模式配置许可服务器。
5. 查看 NetScaler 所需的实例和带宽许可证。
6. 热重启 NetScaler。
7. 在 NetScaler 重新启动后删除固定许可。

CICO 到灵活许可

适用于 **VPX**

1. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
2. 使用 NetScaler GUI 删除现有许可证服务器。在所有步骤完成之前，NetScaler 是未经许可的。
3. 使用灵活/池化选项添加许可证服务器。
4. 查看 NetScaler 所需的实例和带宽许可证。
5. 热重启 NetScaler。

自管理带宽许可证到灵活许可

有些步骤在 MPX、SDX 和 VPX 中很常见。首先列出这些步骤，然后是特定于 MPX、SDX 或 VPX 的步骤。

VPX/MPX/SDX 的常见步骤

1. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
2. 如果您拥有在特定时期内有效的 Z-Cap 软件许可证，请在 NetScaler 硬件 (MPX/SDX) 上申请该许可证。

适用于 **VPX/MPX**

1. 如果您拥有自助管理 Premium 许可证，请使用 NetScaler GUI 将许可模式从自助管理池更改为灵活/池化。
2. 不需要重启 NetScaler。
3. 如果您拥有自我管理的标准版或高级版许可，请使用 NetScaler GUI 删除现有许可服务器。
4. 使用灵活/池化选项添加许可证服务器。
5. 查看 VPX/MPX 的灵活 Premium 带宽容量。
6. 热重启 NetScaler。

适用于 **SDX**

1. 如果 SDX 上的所有 VPX 都有自助管理 Premium 许可，请使用 NetScaler GUI 将许可模式从自助管理池更改为灵活/池化。
2. 不需要重启 NetScaler。
3. 如果 SDX 上的某些 VPX 具有自我管理的标准版或高级版许可，请联系 Citrix 支持部门。

自管理 **vCPU** 到灵活许可

适用于 **VPX**

1. 在 NetScaler 控制台上上载并应用灵活许可。请参阅许可证文件。
2. 使用 NetScaler GUI 删除现有许可证服务器。在所有步骤完成之前，NetScaler 是未经许可的。
3. 使用灵活/池化选项添加许可证服务器。
4. 查看 NetScaler 所需的实例和带宽许可证。
5. 热重启 NetScaler。

合并容量

January 29, 2024

NetScaler 中的池容量是一个许可框架，它包括在 NetScaler 控制台上托管和服务的公共带宽和实例池。您的数据中心中的每个 NetScaler 实例（无论平台或尺寸规格如何）都从此公用池中签出一个实例许可证和仅所需的带宽。许可证

文件和带宽未绑定到实例。当实例不再需要这些资源时，就会将其重新签入公用池，以使资源可用于需要它们的其他实例。

> 注意
>
> 在 NetScaler 控制台中，其中一个代理是许可服务器。

此许可框架通过确保为实例分配的带宽不超过其要求，最大限度地提高了带宽利用率。NetScaler 实例能够检查公共池中的许可和带宽，这也使您能够自动配置实例。

您可以在运行时增加或减少分配给实例的带宽，而不会影响流量。您还可以将池中的许可证从一个实例传输到另一个实例。

配置池化容量

January 29, 2024

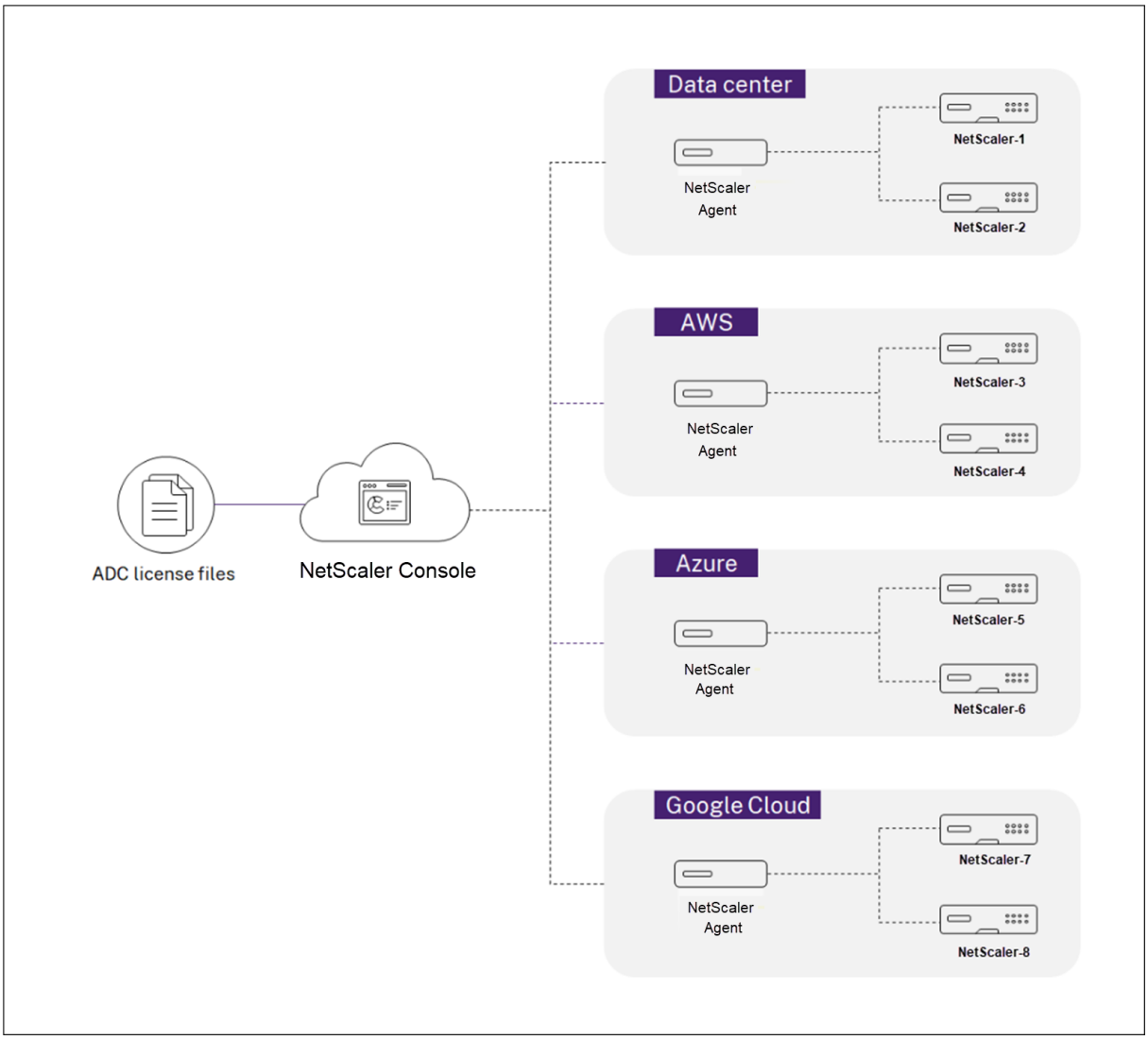
NetScaler 池容量允许您在不同的 NetScaler 外形规格之间共享带宽或实例许可。对于基于虚拟 CPU 订阅的实例，您可以跨实例共享虚拟 CPU 许可证。将此池化容量用于数据中心或公有云中的实例。当实例不再需要资源时，它会将分配的容量重新检查到公用池中。将释放的容量重复使用给其他需要资源的 NetScaler 实例。

您可以使用池化许可确保为实例分配必要的带宽，但不超过其需求，从而最大限度地提高带宽利用率。在不影响流量的情况下，增加或减少在运行时分配给实例的带宽。使用池化容量许可证，您可以自动配置实例。

要使用 NetScaler 池容量，必须将 NetScaler 控制台代理连接到 NetScaler 实例。NetScaler 实例通过代理从 NetScaler 控制台签入和签出许可。

您还可以为 NetScaler FIPS 实例使用池化容量许可。您可以在 NetScaler 控制台中执行以下任务：

1. 将池容量许可证文件（带宽池或实例池）上载到许可证服务器。
2. 根据需要将许可证池中的许可证分配给 NetScaler 实例。
    - 根据实例的最小和最大容量查看 NetScaler 实例（MPX-Z /SDX-Z/VPX/CPX/BLX）的许可证。



您可以从 citrix.com 下载池化许可证，包括带宽、实例和 Z-cap 许可证。有关更多信息，请参阅 NetScaler 许可指南。

NetScaler 池容量问题

池化容量状态指示 NetScaler 实例的许可要求。使用池化容量配置的 NetScaler 实例显示以下状态之一：

- 最佳：实例以适当的许可证容量运行。
- 容量不匹配：实例的运行容量小于用户配置的容量。
- 宽限：实例正在使用宽限许可证运行。
- 宽限期和不匹配：实例在宽限期运行，但容量小于用户配置的容量。
- 不可用：实例未在 NetScaler 控制台中注册以进行管理，或者从 NetScaler 控制台到实例的 NITRO 通信不起作用。

- 未分配：未在实例中分配许可证。

开始之前的准备工作

在配置池化容量之前，请确保以下几点：

- 在 NetScaler 控制台中安装和注册代理。要安装和注册代理，请参阅 入门。
- 确保所有注册代理都处于 UP 状态，以便池化许可正常运行。如果代理处于 DOWN 状态但尚未停用或终止，请将其置于 UP 状态。如果 DOWN 代理已停用、终止或不再使用，请将其从 NetScaler 控制台中删除。
- 27000和 7279端口可用于将许可从 NetScaler 控制台签出到实例。请参阅“系统要求”。

第 **1** 步-在 **NetScaler** 控制台中申请许可

1. 在 NetScaler 控制台中，导航 到基础架构 **>** 池化许可。
2. 在“许可证文件”部分中，选择“添加许可证文件”，然后选择以下选项之一：
   - 从本地计算机上载许可证文件。如果您的本地电脑上已经存在许可文件，则可以将其上载到 NetScaler 控制台。
   - **Use license access code**（使用许可证访问代码）。为您从 Citrix 购买的许可证指定许可证访问代码。然后，选择 获取许可证。然后选择完成。

   > 注意：
   >
   > 您可以随时从“许可设置”向 NetScaler 控制台添加更多许可。

3. 单击完成。

   许可文件将添加到 NetScaler 控制台中。许可到期信息选项卡列出了 NetScaler 控制台中存在的许可以及剩余的到期天数。

4. 在 许可证文件中，选择要应用的许可证文件，然后单击 应用许可证。

   此操作允许 NetScaler 实例使用所选许可作为池化容量。

第 **2** 步-将 **NetScaler** 控制台注册为许可服务器

您可以使用代理将 NetScaler 控制台注册为 NetScaler 实例的许可服务器。

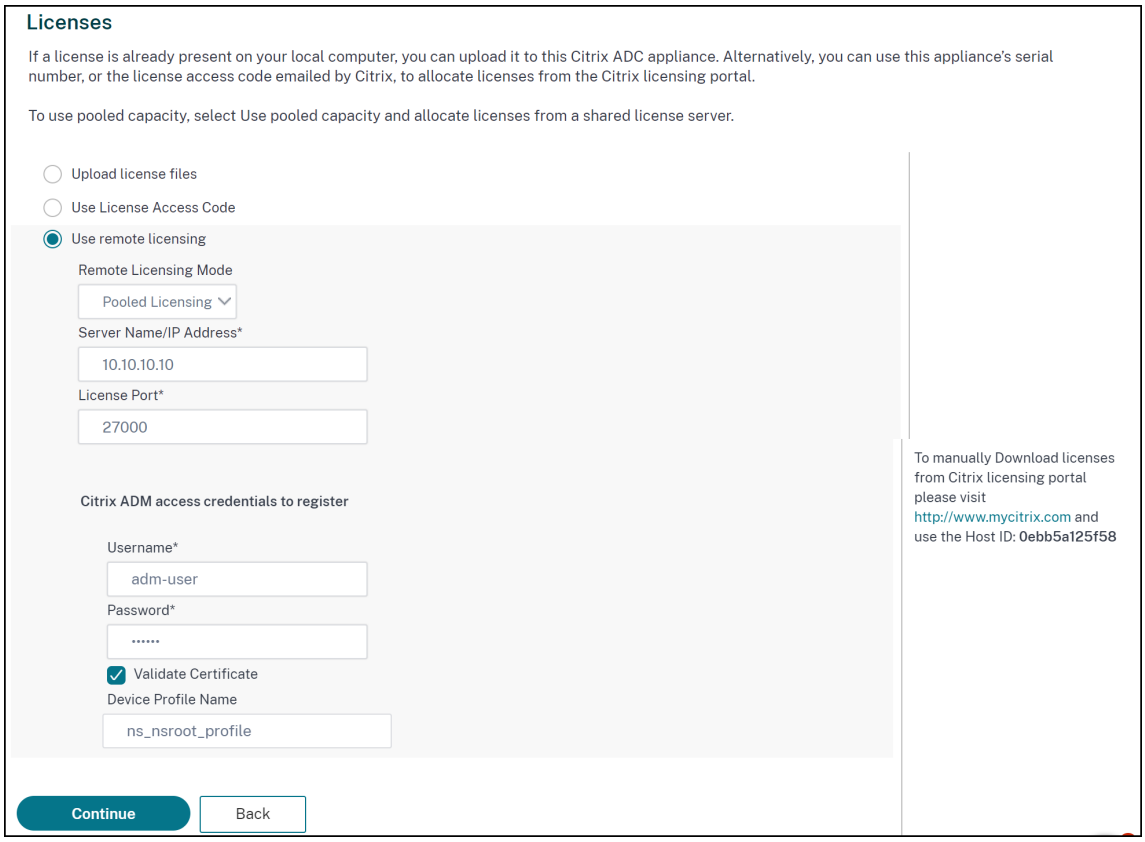
使用以下步骤之一将 NetScaler 控制台注册为许可服务器：

- 使用图形用户界面

使用 **GUI** 注册代理

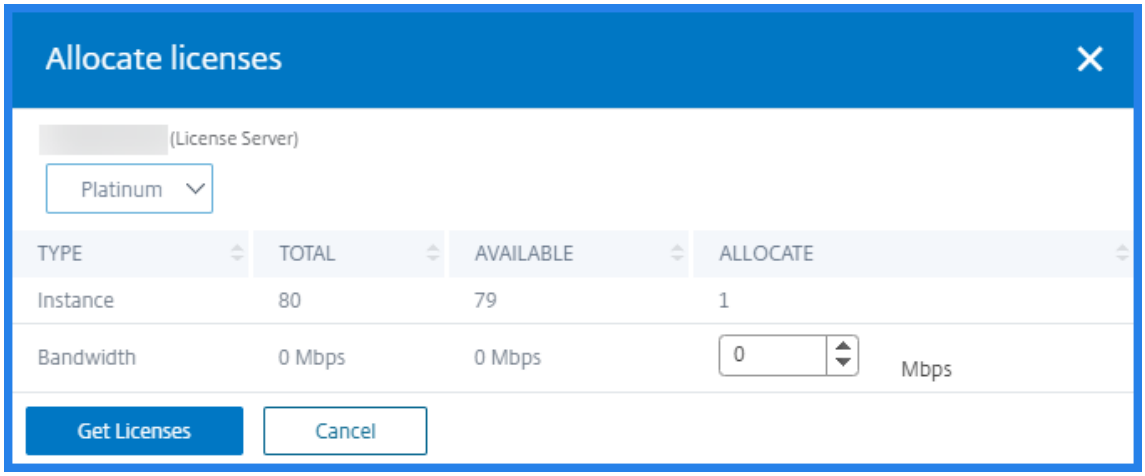
在 NetScaler 控制台 GUI 中，注册与 NetScaler 实例关联的代理。

1. 登录到 NetScaler GUI。
2. 导航到“系统”>“许可证”>“管理许可证”。
3. 单击“添加新许可证”。
4. 选择 使用远程许可，然后从列表中选择远程许可模式。
5. 在“服务器名称/**IP** 地址”字段中，指定在 NetScaler 控制台中注册的关联代理的 IP 地址。
6. 选择“向 **NetScaler** 控制台注册”。
7. 输入您的代理凭据以在 NetScaler 控制台注册实例，然后单击“继续”。在 NetScaler 控制台中，其中一个代理是许可服务器。



8. 在 分配许可证中，选择许可证版本并指定所需的带宽。

   首次在 NetScaler 中分配许可证。稍后您可以通过 NetScaler 控制台 GUI 更改或释放许可分配。



9. 单击 **Get Licenses**（获取许可证）。

> 重要
>
> 如果您更改了许可证版本，请热重启实例。在您重新启动实例之前，配置更改才会生效。

使用 **CLI** 添加代理

如果 NetScaler 实例没有 GUI，请使用以下 CLI 命令添加与实例关联的代理：

1. 登录 NetScaler 控制台。
2. 添加在 NetScaler 控制台中注册的关联代理的 IP 地址：

```
1 > add ns licenseserver <adm-agent-IP-address> -port <adm-agent-
    license-port-number>
```

3. 查看许可证服务器中可用的许可证带宽：

```
1 > sh ns licenseserverpool
```

4. 从所需的许可证版本中分配许可证带宽：

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
```

许可证版本可以是标准版本、高级或高级版。

> 重要信息：如果您更改许可证版本，则“
>
> 热”重新启动实例。
>
> ```
> reboot -w
> ```
>
> 在您重新启动实例之前，配置更改才会生效。

第 3 步-向 NetScaler 实例分配池许可

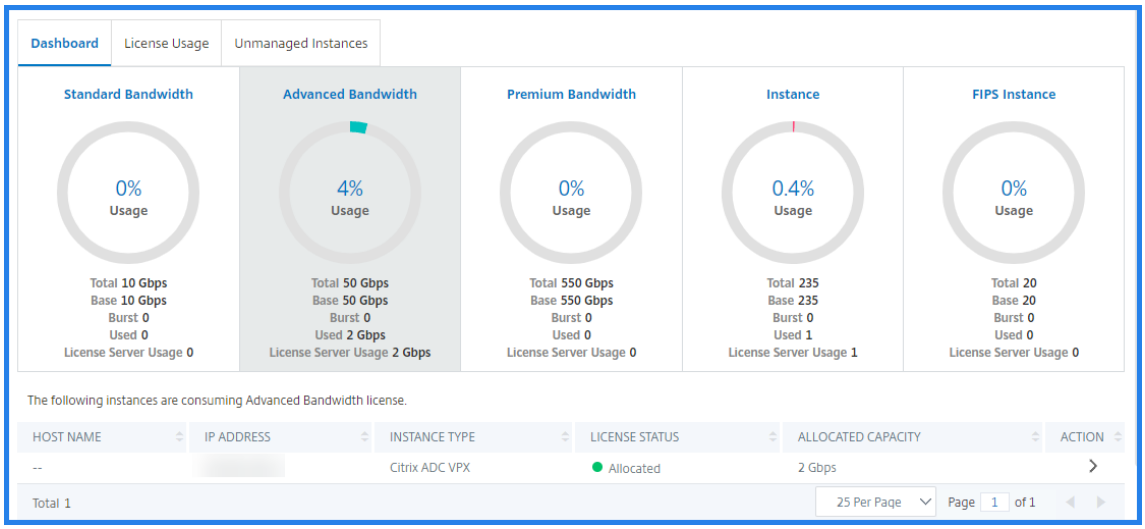
要从 NetScaler 控制台 GUI 中分配池化容量许可，请执行以下操作：

1. 登录 NetScaler 控制台。
2. 导航到 基础结构 > 池化许可 > 带宽许可证 > 池容量。

   只有当您将 FIPS 实例许可上载到 NetScaler 控制台时，才会显示 FIPS 实例容量。
3. 单击要管理的许可证池。

   > 注意：
   >
   > “分配的容量”字段不会立即反映更改的带宽。带宽更改在 NetScaler 热重启后生效。
   >
   > 在 分配详细信息中，当您更改实例的带宽分配时，会更新 请求 和已 应用 字段。

4. 单击 ** 按钮，从可用实例列表中选择 NetScaler 实例。

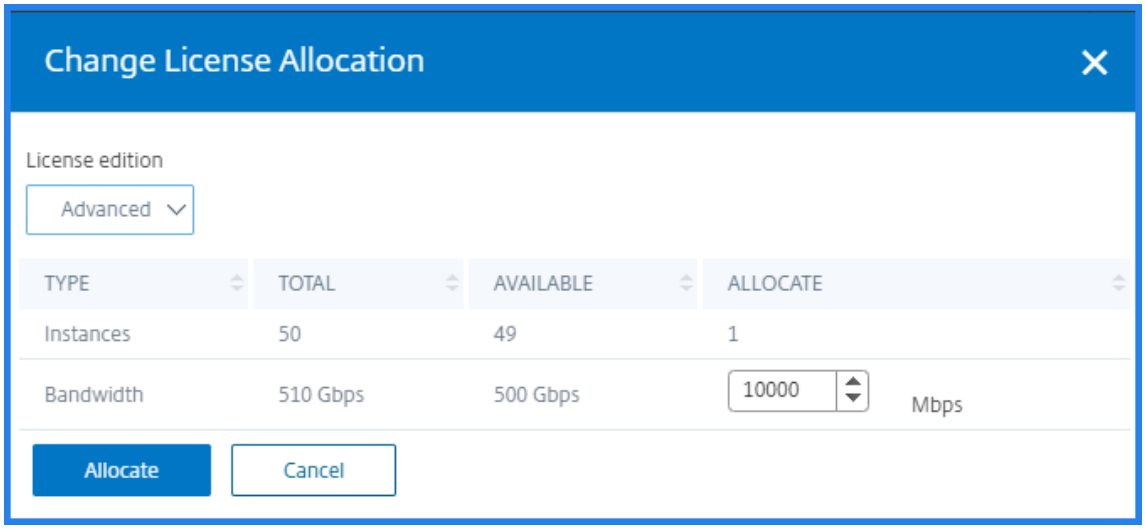


   许可证状态 列显示相应的许可证分配状态消息。

   > 注意：
   >
   > “非托管实例”标签显示已发现但未 在 NetScaler 控制台中管理的实例。

5. 单击“更改分配”或“发布分配”以修改许可证分配。
6. 将出现一个弹出窗口，其中包含许可证服务器中的可用许可证。
7. 您可以通过设置分配列表选项来选择实例的带宽或实例分配。做出选择后，单击“分配”。

8. 您也可以从“更改许可证分配”窗口的列表选项中更改分配的许可证版本。



> 注意：
>
> 如果您更改许可证版本，请热重启实例。

在 **NetScaler** 实例上配置池化容量

您可以在以下 NetScaler 实例上配置池化容量许可：

- NetScaler MPX-Z 实例
- NetScaler SDX-Z 实例
- NetScaler VPX 实例
- NetScaler 高可用性对

NetScaler MPX-Z 实例

MPX-Z 是支持池容量的 NetScaler MPX 设备。MPX-Z 支持高级版、高级版或标准版许可证的带宽池。

MPX-Z 需要许可证才能连接到许可证服务器。您可以使用以下方法之一安装 MPX-Z 许可证：

- 从本地计算机上载许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的“系统”>“许可证”部分中的许可证访问代码。

如果删除 MPX-Z 许可证，则池容量功能将被禁用。实例许可证将释放到许可证服务器。

您可以在不重新启动的情况下动态修改 MPX-Z 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重启实例时，它会自动签出其配置容量所需的池化许可证。

NetScaler SDX-Z 实例

SDX-Z 是支持共享容量的 NetScaler SDX 设备。SDX-Z 支持 Premium、Advanced 或 Standard Edition 许可证的带宽和实例池。

SDX-Z 需要许可证才能连接到许可证服务器。您可以使用以下方法之一安装 SDX-Z 许可证：

- 从本地计算机上载许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的“系统”>“许可证”部分中的许可证访问代码。

如果删除 SDX-Z 许可证，则池容量功能将被禁用。实例许可证将释放到许可证服务器。

您可以在不重启的情况下动态修改 SDX-Z 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重启实例时，它会自动签出其配置容量所需的池化许可证。

NetScaler 实例

启用池容量的 NetScaler VPX 实例可以从带宽池（高级版/高级版/标准版）中检出许可证。您可以使用 NetScaler GUI 从许可服务器签出许可。

您可以在不重新启动的情况下动态修改 VPX 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重启实例时，配置的池化容量许可证将自动从 NetScaler 控制台服务器中签出。

NetScaler 高可用性对

在开始之前，请确保将 NetScaler 控制台服务器配置为许可服务器。有关详细信息，请参见 将 NetScaler 控制台配置为许可服务器

当您为 NetScaler HA 对分配带宽时，NetScaler 控制台会向主实例和辅助实例检出相同的带宽。如果您为 NetScaler HA 对分配 10 Mbps 带宽，NetScaler 控制台将执行以下操作：

1. 检查 HA 对的 20 Mbps 带宽。
2. 为 HA 对中的每个实例分配 10 Mbps。

要向 NetScaler HA 对分配池许可，请参见向 NetScaler 实例分配池许可。

池容量 页面分别显示实例及其分配的容量。如果您更改或释放主实例的带宽，则辅助实例带宽会自动与主实例同步。但是，如果您更改或释放辅助实例带宽，则不会发生同步。

将 **NetScaler MPX** 中的永久许可证升级到 **NetScaler** 池容量

January 29, 2024

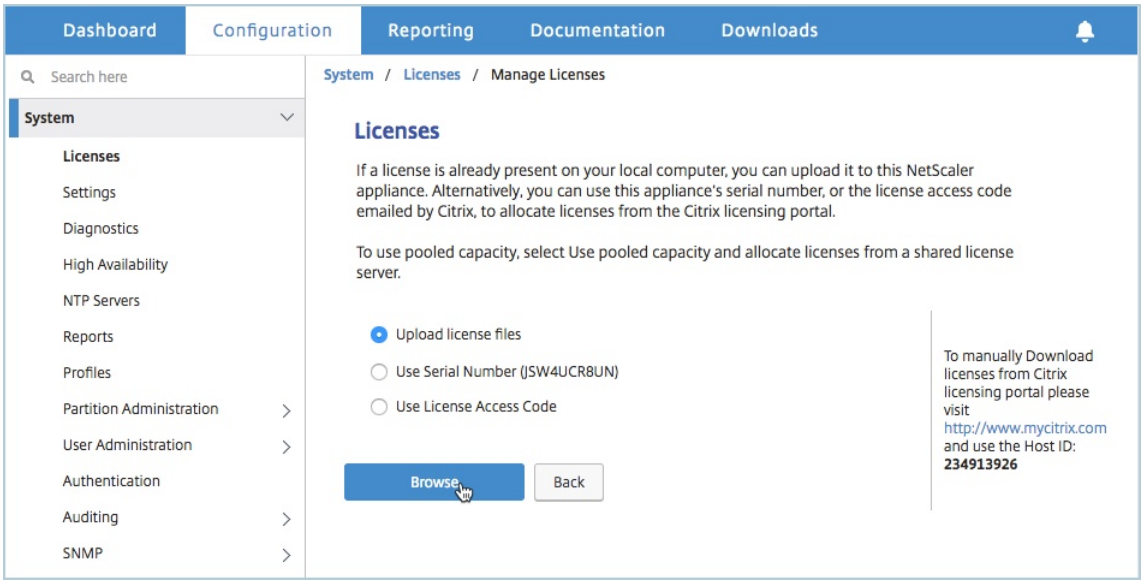
具有永久许可证的 NetScaler MPX 设备可以升级到 NetScaler 池容量许可证。升级到 NetScaler 池容量许可使您能够根据需要将许可池中的许可分配给 NetScaler 设备。NetScaler 一次只能使用一个许可证，即使用永久许可证或使用池化许可证。客户可以从共用许可证切换到永久许可证。只要永久许可证有效，您就可以重新配置 NetScaler 并删除池化许可证配置。当客户从永久许可证切换到池化许可证或从池化许可证切换到永久许可证时，所有 NetScaler 实例都将重新启动。

您还可以为在高可用性模式下配置的 NetScaler 实例配置 NetScaler 池容量许可。要在高可用模式下为 NetScaler MPX 实例配置 NetScaler 池容量许可证，请参阅将 NetScaler MPX 高可用性对中的永久许可证升级为 NetScaler MPX 池容量。

> 注意
>
> 要将 NetScaler MPX 设备升级到 NetScaler 池容量许可，您需要将 MPX-Z 许可上载到该设备。

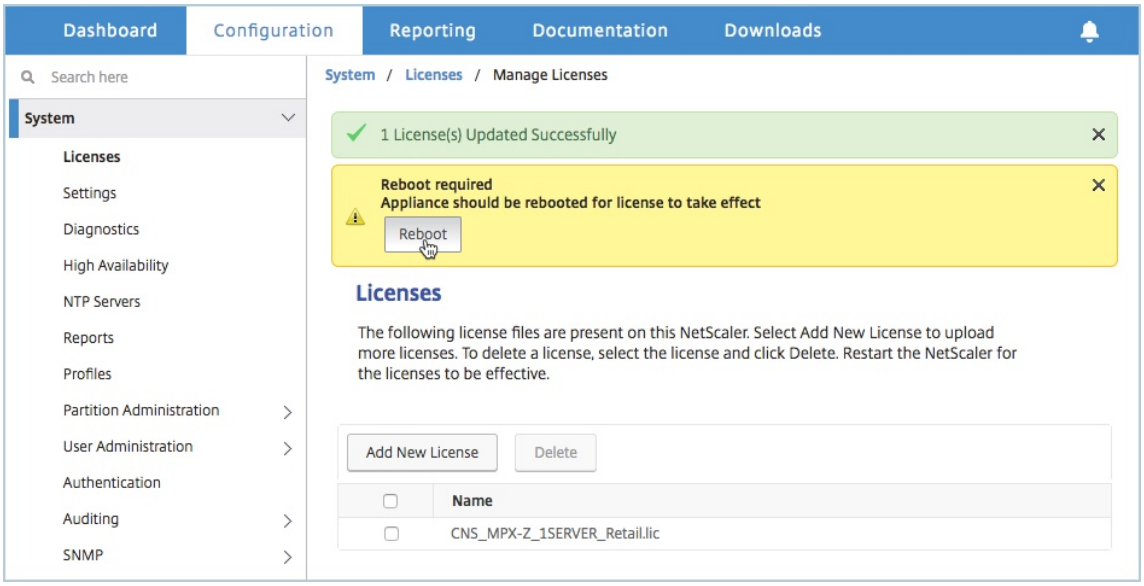
要升级到 **NetScaler** 池容量，请执行以下操作：

1. 在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 上载零容量许可证（MPX-Z 许可证）。在配置选项卡上，导航到 系统 > 许可证。
5. 在详细信息窗格中，单击“管理许可证”，单击“添加 新许可证”。
6. 在“许可证”页面中，选择“上载许可证文件”，然后单击“浏览”从本地计算机中选择零容量许可证。

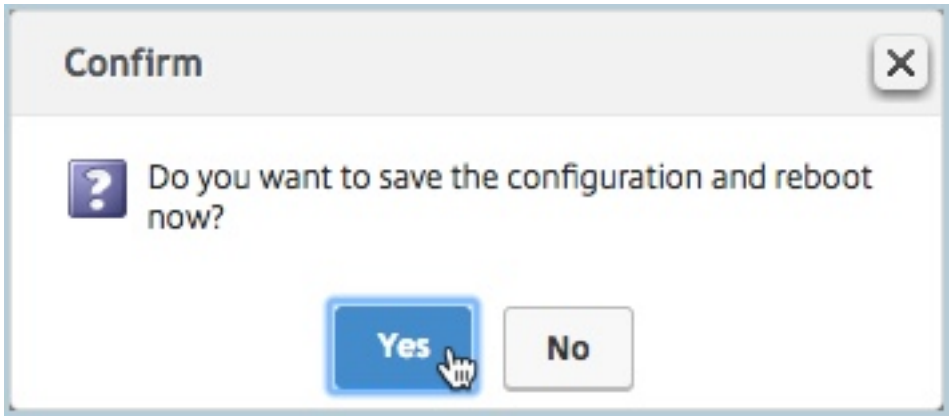


7. 上载许可证后，单击 重新启动 以重新启动设备。

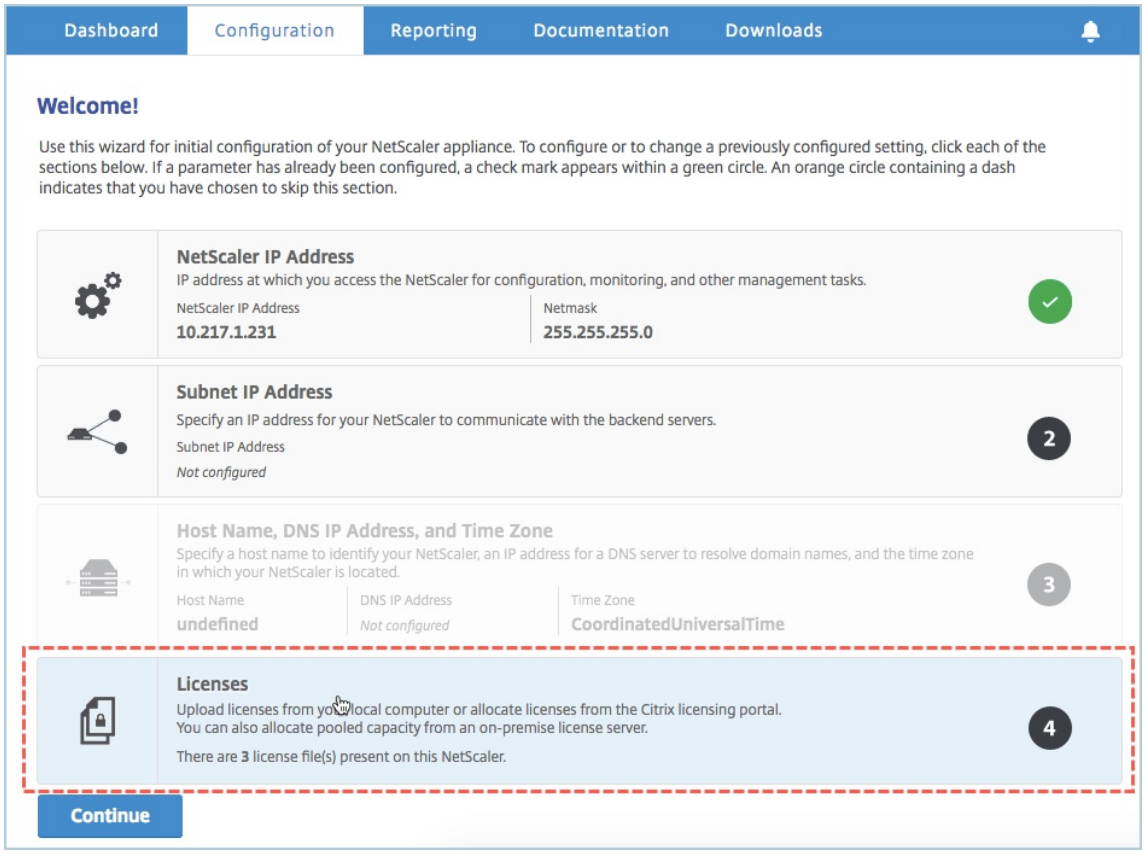
> 警告应用 MPX-Z 许可证
>
> 后，装置上包括 SSL 卸载在内的功能将变为未授权。设备停止处理 HTTPS 请求。
>
> 如果在升级之前在设备上启用了“仅限安全访问”选项，则无法使用 HTTPS 通过 NetScaler 控制台 GUI 连接到该设备。



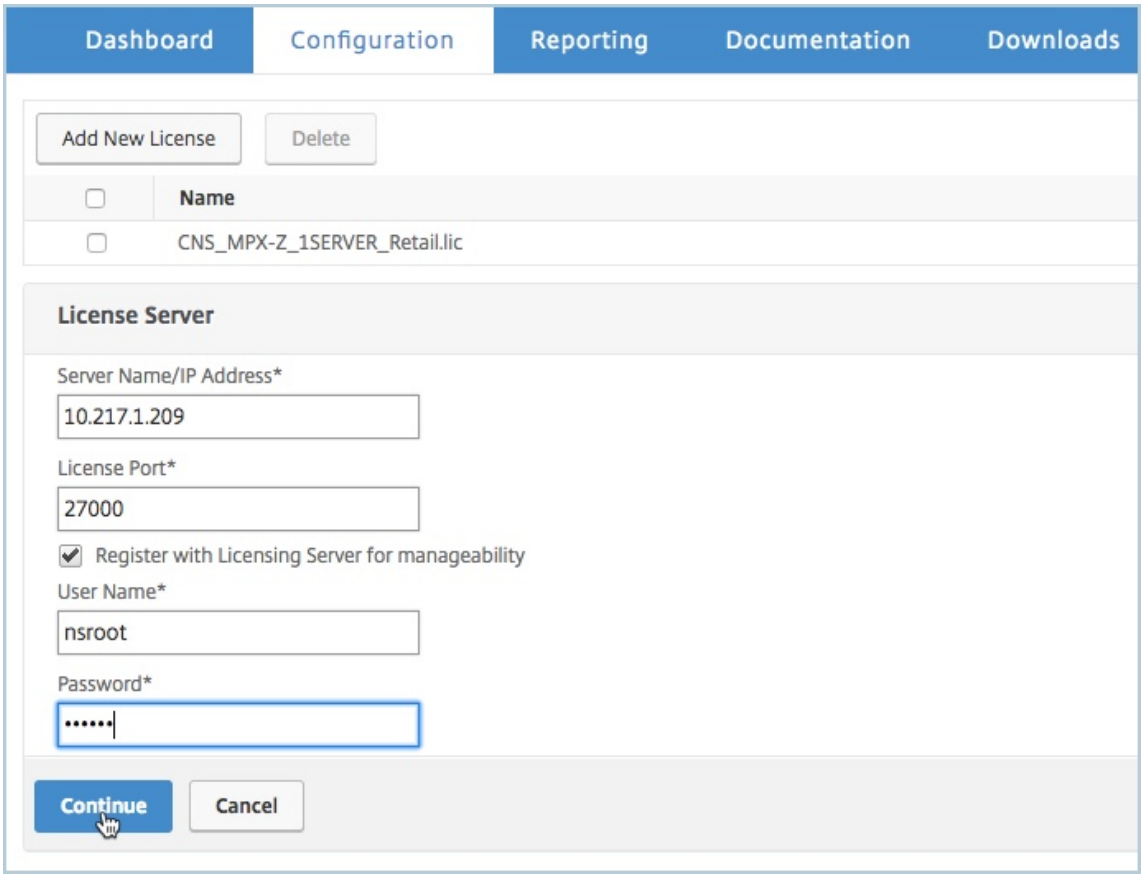
8. 在“确认”页上，单击“是”。



9. 装置重新启动后，登录到装置。
10. 在“欢迎”页面上，单击“许可证”部分。



11. 在“许可证服务器”部分中，执行以下操作：



a) 在“服务器名称 **/IP** 地址”字段中，输入许可证服务器详细信息。

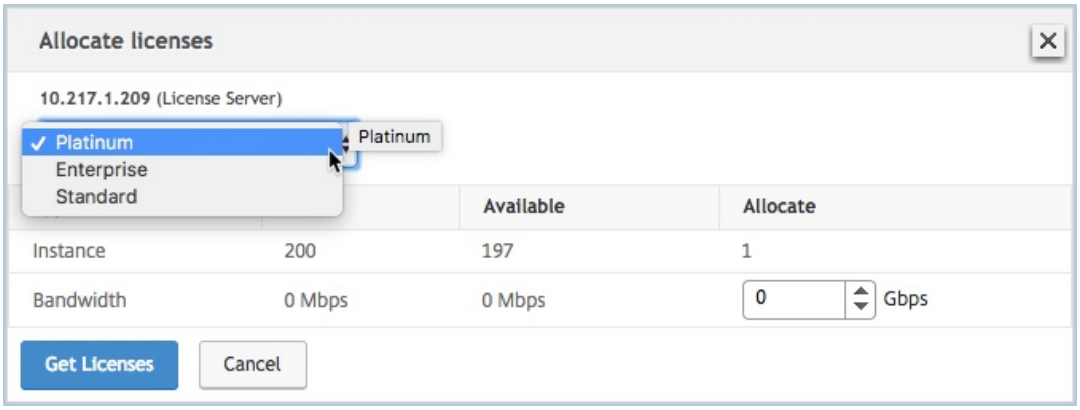
b) 在 许可证端口 字段中，输入许可证服务器端口。默认值：27000。

c) 如果您想通过 NetScaler 控制台管理实例的池许可，请选中“向 许可服务器注册以实现可管理性”复选框并输入 NetScaler 控制台凭 据。

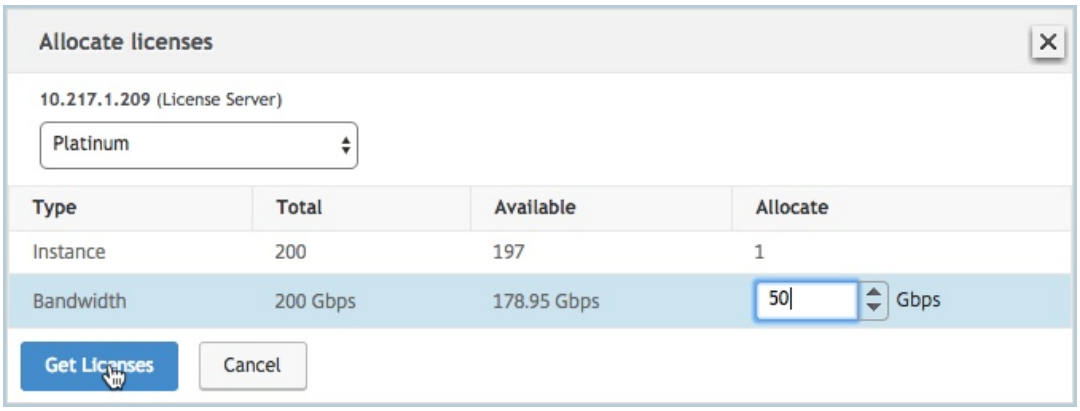
d) 单击继续。

12. 在“分配许可证”窗口中，执行以下操作：

a) 从下拉列表中选择许可证版本。

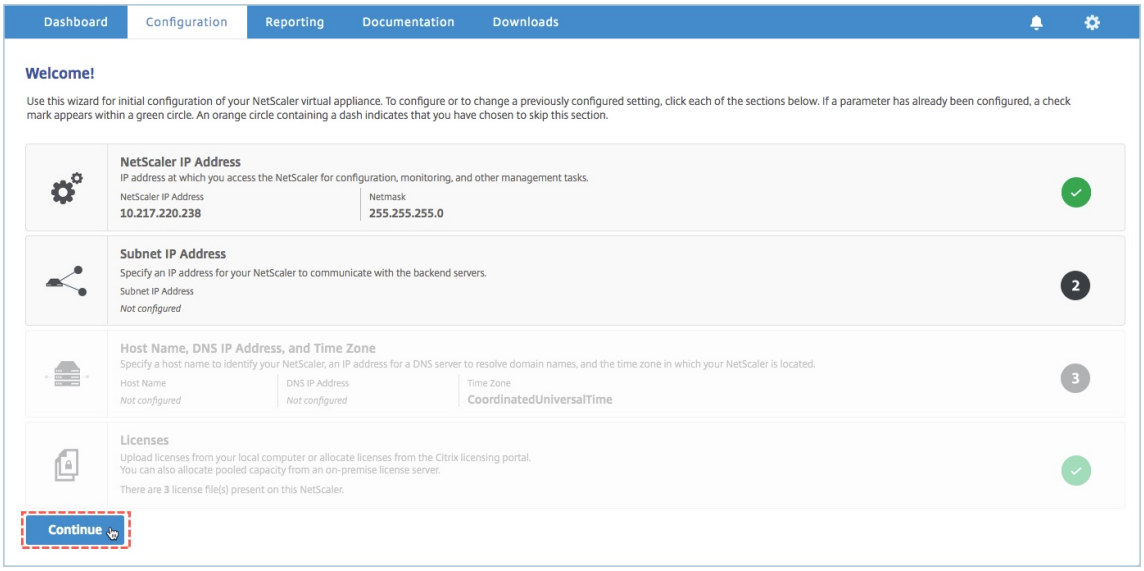


b) 从“分配”菜单将带宽分配 给 NetScaler 装置，然后单击“获取许可证”。

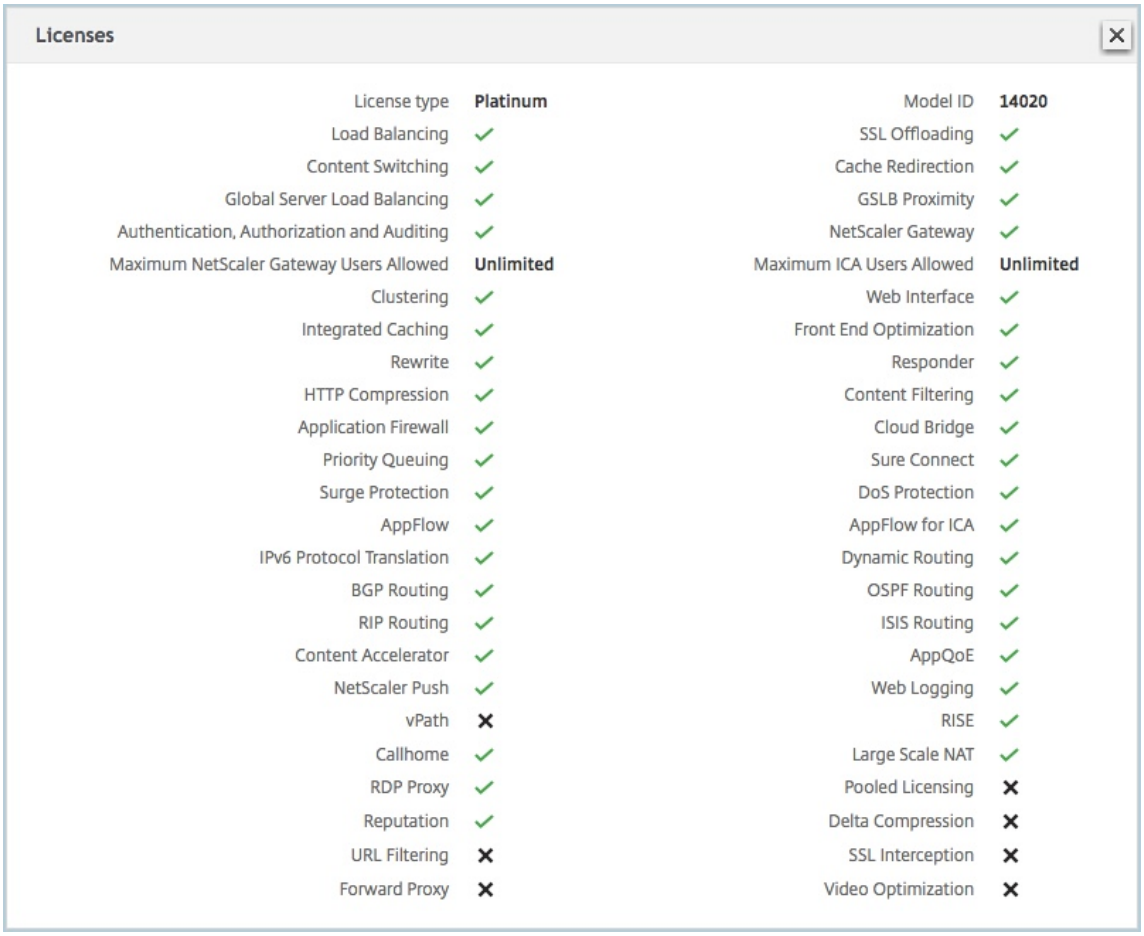


c) 出现提示时，单击 重新启动 以重新启动装置。

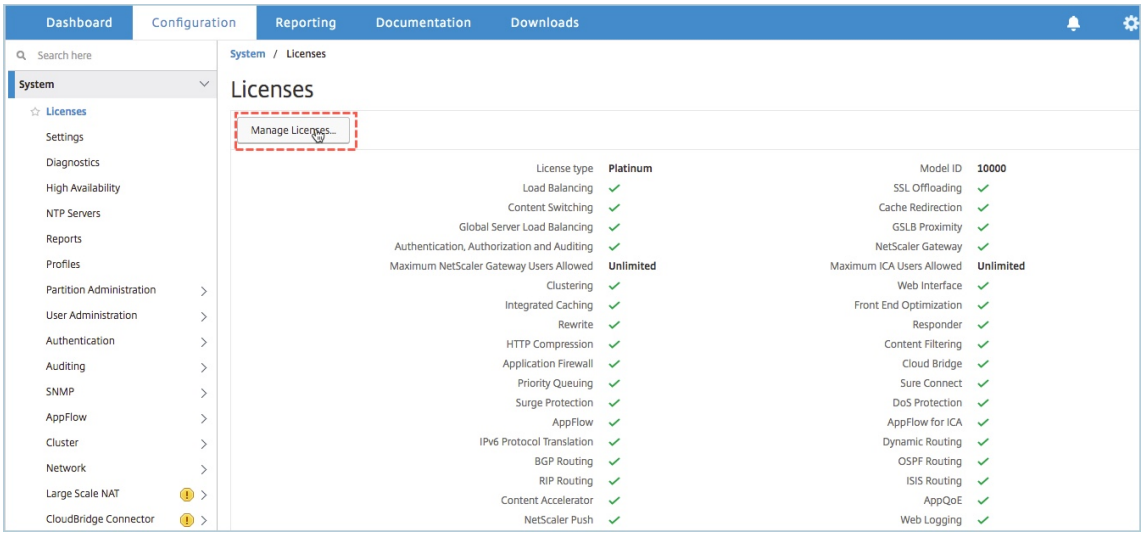
13. NetScaler MPX 设备重新启动后，登录 NetScaler MPX 设备。在“欢迎 使用”页面上，单击“继续”。



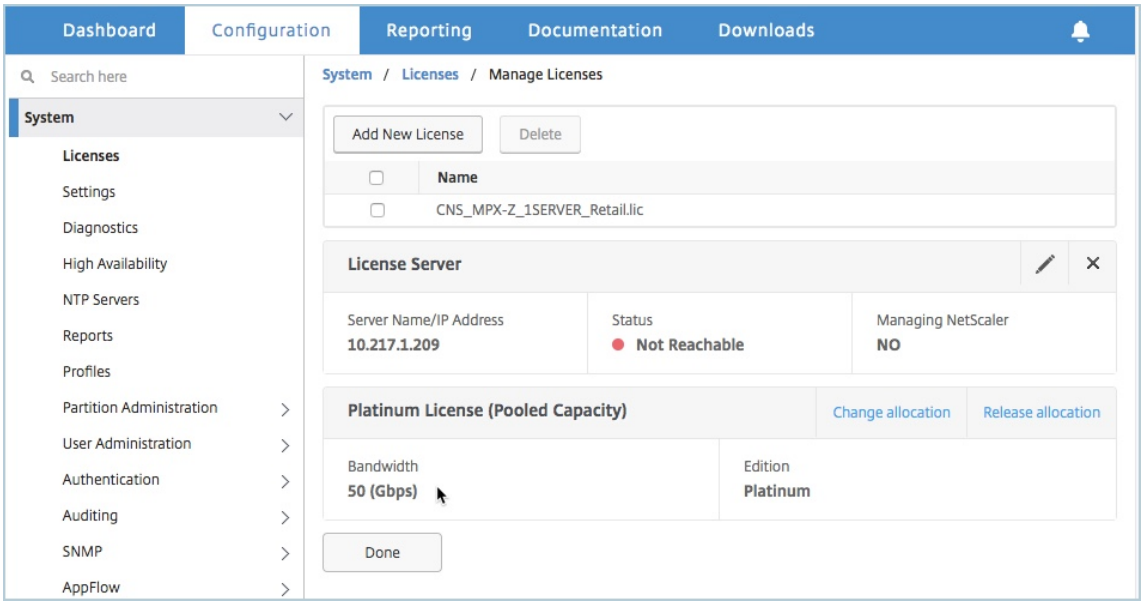
“许可证”页面列出了所有已许可的功能。



14. 导航到“系统”**>**“共享许可”，然后单击“管理许可证”。



在“管理许可证”页面上，可以查看许可证服务器、许可证版本和分配带宽的详细信息。



将 **NetScaler MPX** 高可用性对中的永久许可证升级到 **NetScaler** 池容量

对于配置为高可用模式的 NetScaler MPX 设备，必须在 HA 对中的主实例和辅助 NetScaler 实例上配置 NetScaler 池容量。您需要将相同容量的许可证分配给 HA 对中的主 NetScaler 实例和辅助实例。例如，如果您想让 HA 对中的每个实例获得 1 Gbps 的容量，则需要从公用池中分配 2 Gbps 的容量，这样您就可以为 HA 对中的主和辅助 NetScaler 实例各分配 1 Gbps 的容量。

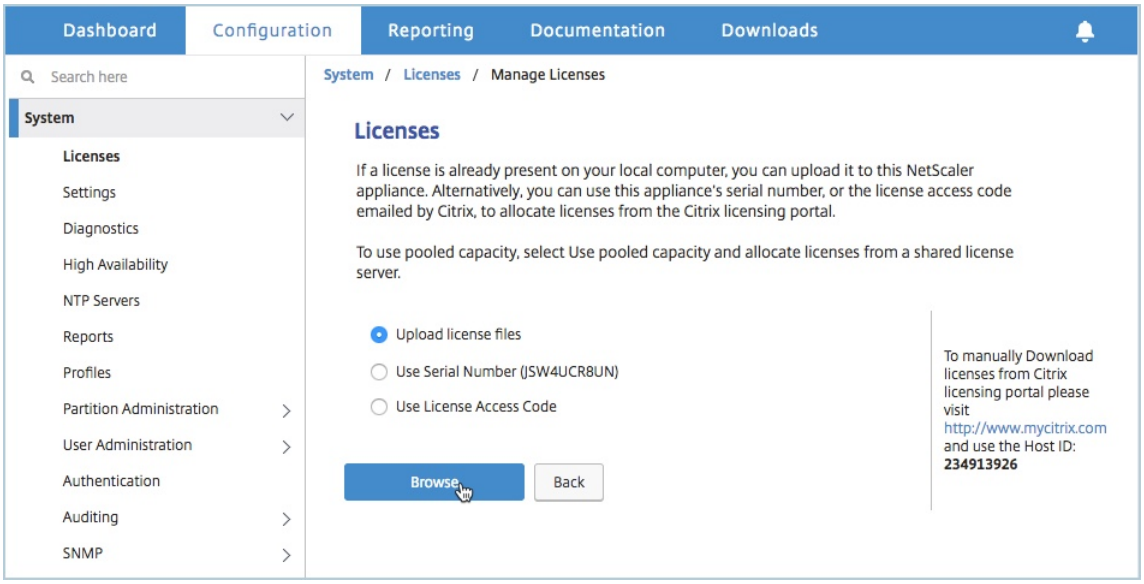
> 重要
>
> 要将 NetScaler MPX 设备升级为使用 NetScaler 池容量许可，需要将 MPX-Z 上载到该设备。

必备条件

确保将 MPX-Z 许可证上载到 HA 对中的主实例和辅助实例。

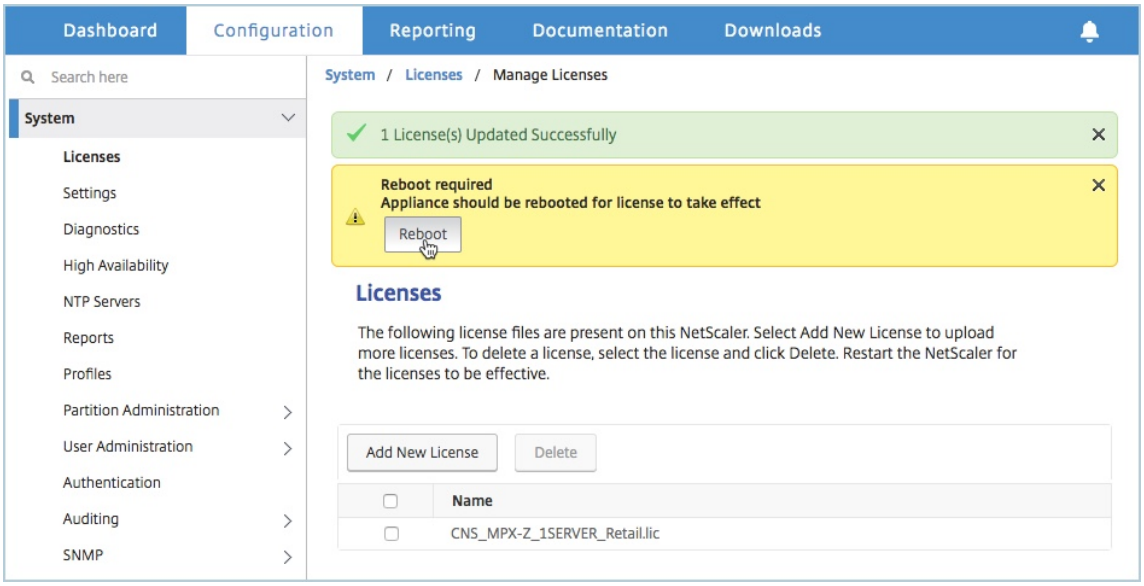
要将 **MPX-Z** 许可证上载到 **HA** 对中的 **NetScaler MPX** 实例，请执行以下操作：

1. 在 Web 浏览器中，键入设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 上载零容量许可证（MPX-Z 许可证）。在 **Configuration**（配置）选项卡上，导航到 **System**（系统）> **Licenses**（许可证）。
5. 在详细信息窗格中，单击“管理许可证”，单击“添加新许可证”。
6. 在“许可证”页面中，选择“上载许可证文件”，然后单击“浏览”从本地计算机中选择零容量许可证。

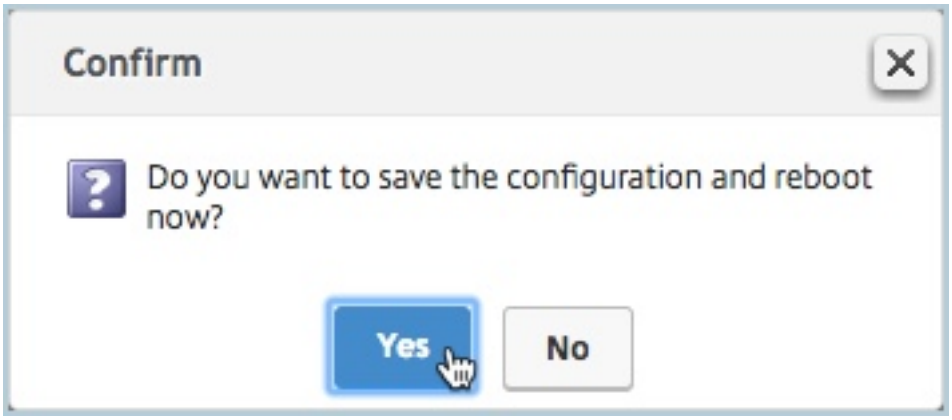


上载许可证后，系统会提示您重新启动设备。

7. 单击“重新启 动”以重新启动装置。

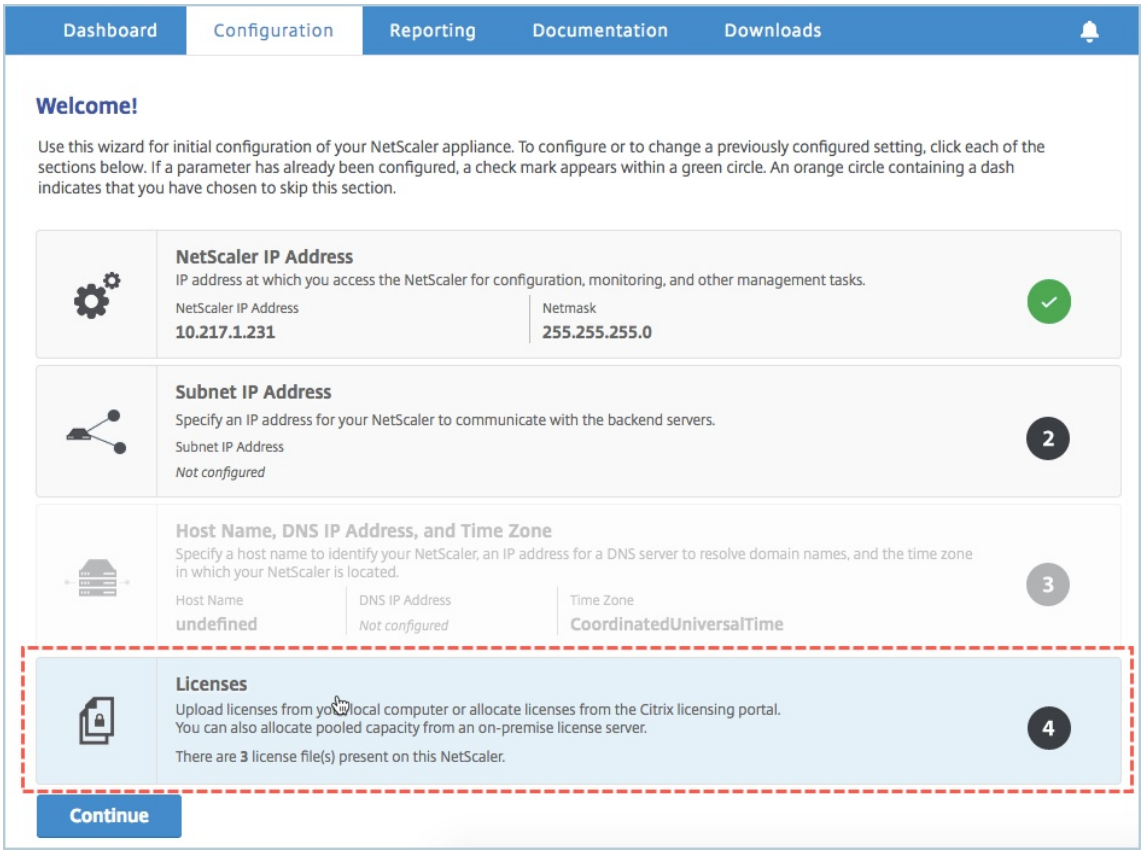


8. 在“确认”页上，单击“是”。

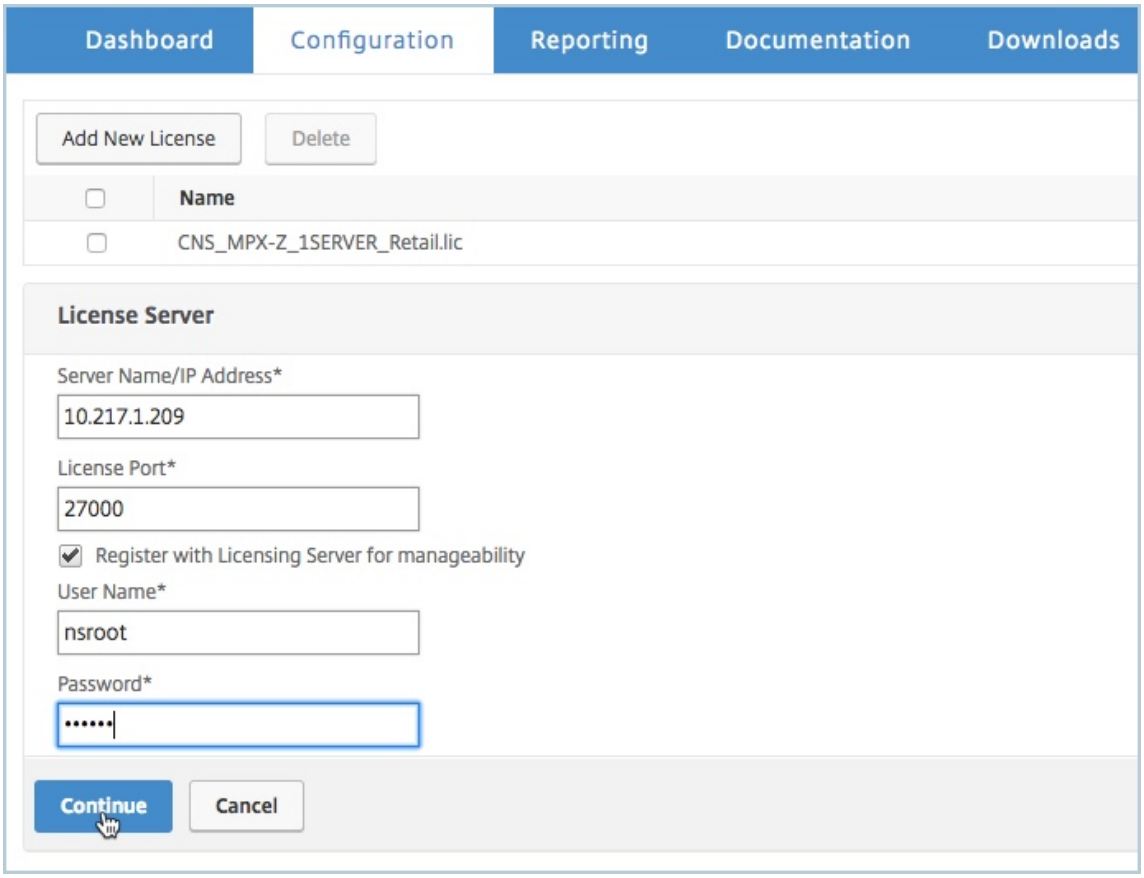


要将现有 **HA** 设置升级到 **NetScaler** 池容量，请执行以下操作：

1. 登录到辅助 NetScaler MPX 实例。在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎”页面上，单击“许可证”部分。



4. 在“许可证服务器”部分中，执行以下操作：



a) 在“服务器名称 **/IP** 地址”字段中，输入许可证服务器详细信息。

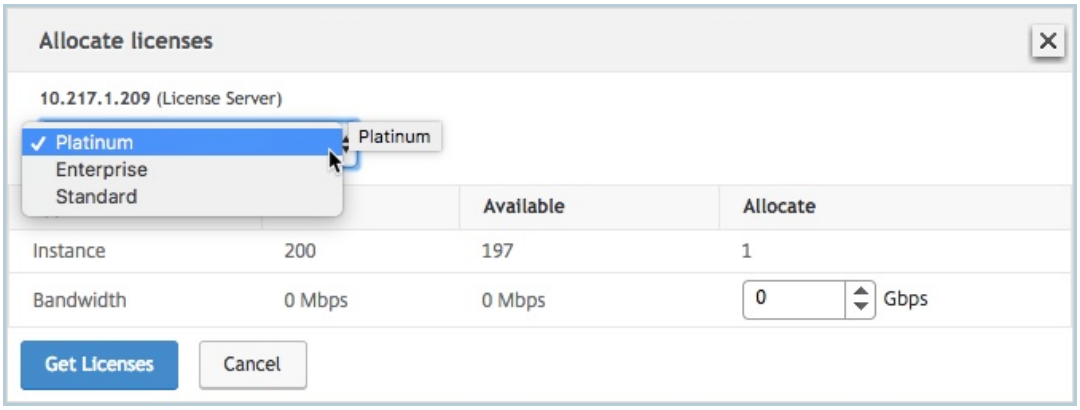
b) 在 许可证端口 字段中，输入许可证服务器端口。默认值：27000。

c) 如果您想通过 NetScaler 控制台管理实例的池许可，请选中“向 许可服务器注册以实现可管理性”复选框并输入 NetScaler 控制台凭 据。

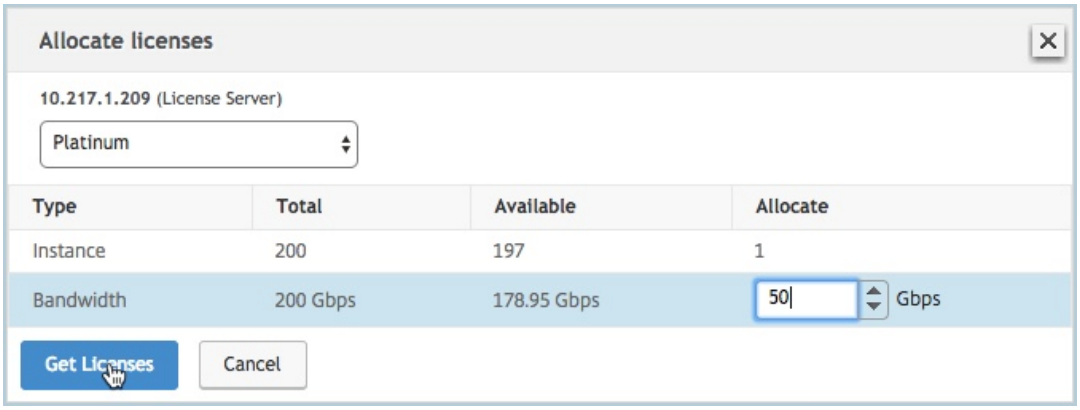
d) 单击继续。

5. 在“分配许可证”窗口中，执行以下操作：

a) 从下拉列表中选择许可证版本。



b) 从“分配”菜单将带宽分配 给 NetScaler 装置，然后单击“获取许可证”。



c) 出现提示时，单击 重新启动 以重新启动装置。

辅助 NetScaler MPX 装置重新启动后，它将成为 HA 对中的主 NetScaler MPX 装置。

6. 登录现有主 NetScaler MPX 设备并重新启动设备。执行以下操作：

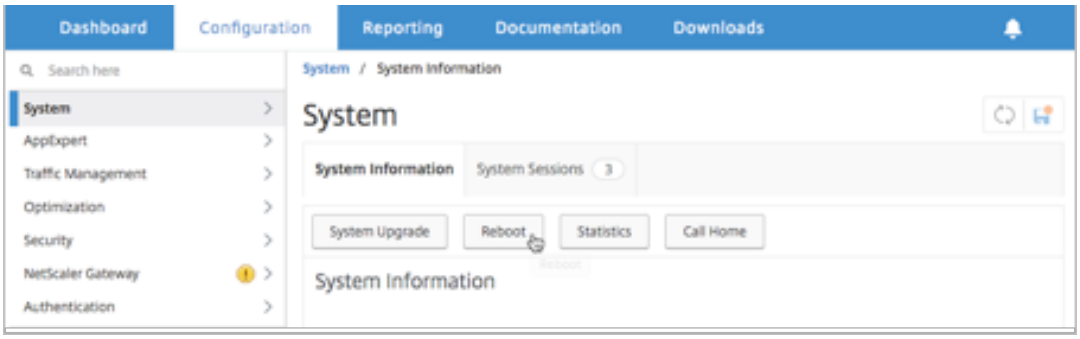
a) 在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 http://192.168.100.1。

b) 在“用户名”和“密码”字段中，键入管理员凭据。

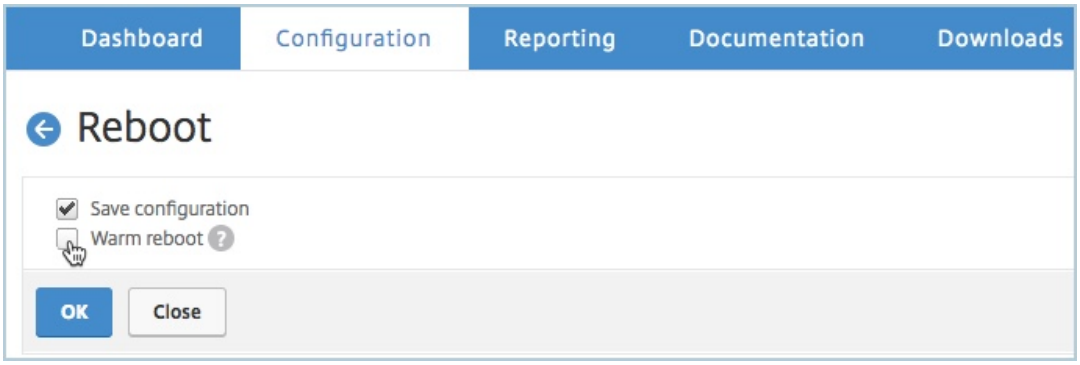
c) 在“欢迎 使用”页面上，单击“继续”。

d) 在“配置”选项卡上，单击“系统”。

e) 在“系统”页面上，单击“重新启动”。



f) 在“重新启动”页面上，选择“热重新启动”，然后单击“确定”。



主 NetScaler MPX 装置重新启动后，它将成为 HA 对中的辅助 NetScaler MPX 装置。如果需要，您可以在 HA 对中的任何实例上使用以下命令将 HA 对中的主实例和辅助实例更改为原始 HA 对配置：

```
1 > force ha failover
```

将 **NetScaler SDX** 中的永久许可证升级到 **NetScaler** 池容量

January 29, 2024

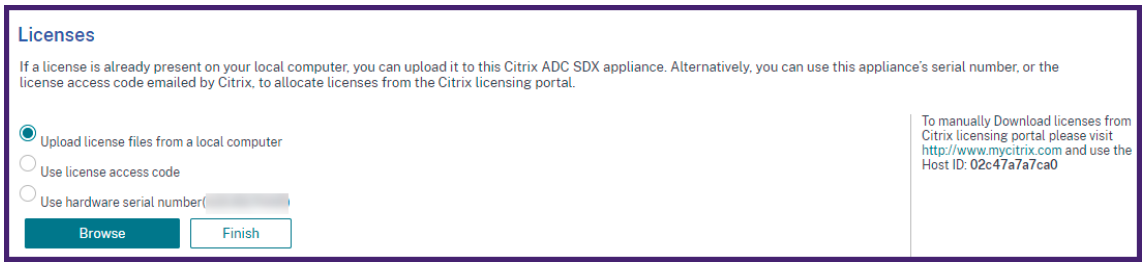
具有永久许可证的 NetScaler SDX 可以升级到 NetScaler 池容量许可证。升级到 NetScaler 池容量许可使您能够根据需要将许可池中的许可分配给 NetScaler 设备。NetScalerCan 一次只能使用一个许可证，即使用永久许可证或使用池化许可证。客户可以从池化许可证切换到永久许可证。只要永久许可证有效，客户就可以重新配置 NetScaler 并删除池化许可证配置。当客户从永久许可证切换到池化许可证或从池化许可证切换到永久许可证时，所有 NetScaler 实例都将重新启动。

您还可以为在高可用性模式下配置的 NetScaler 实例配置 NetScaler 池容量许可。

> 注意
>
> 要将 SDX 设备升级到 NetScaler 池容量许可，必须将 SDX-Z 许可上载到该设备。
>
> 确保您有权在 NetScaler 控制台中添加 NetScaler 实例。

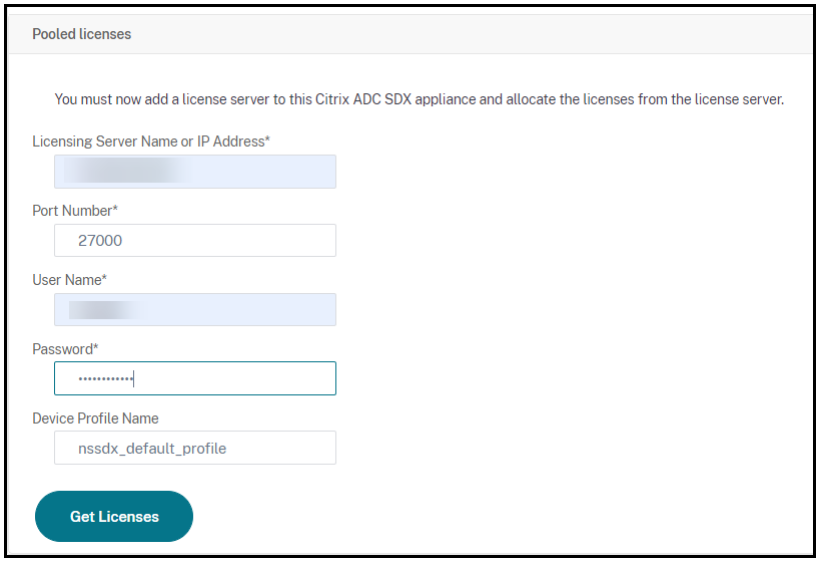
要升级到 **NetScaler** 池容量，请执行以下操作：

1. 在 Web 浏览器中，键入 SDX 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 上载零容量许可证。在配置选项卡上，导航到 系统 > 许可证。
5. 在“管理许可证”页面上，单击“添加许可证文件”。
6. 在“许可证”页面中，选择“从本地计算机上载许可证文件”，然后单击“浏览”从本地计算机中选择零容量许可证。然后，单击“完成”。



成功应用零容量许可证后，“许可证”页面上会显示“池化许可 证”部分。

7. 在 池许可证部 分中，执行以下操作：



a) 在 授权服务器名称或 **IP** 地址 字段中，输入许可证服务器详细信息。

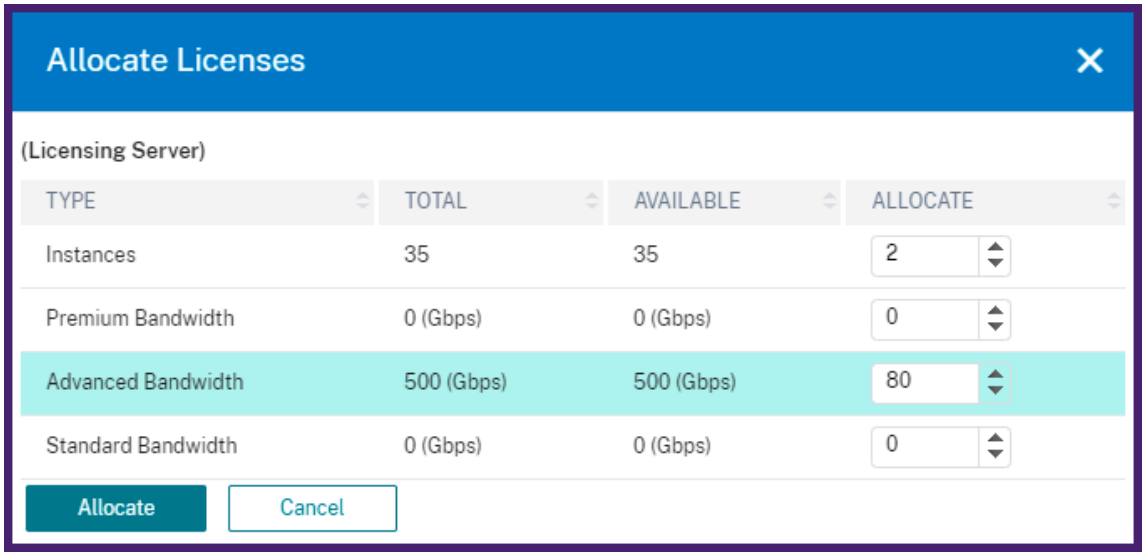
如果要将 NetScaler 控制台服务器配置为许可服务器，请指定 NetScaler 控制台服务器的 IP 地址。

如果您使用代理与 NetScaler 控制台服务器通信，请指定该代理的 IP 地址。

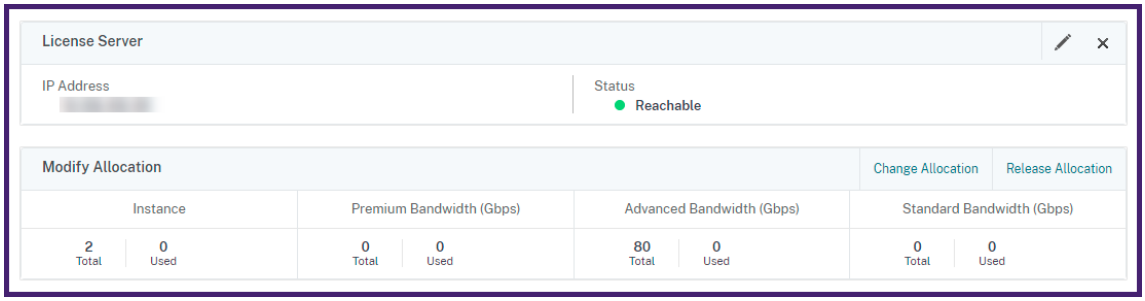
b) 在 端口号 字段中，输入许可证服务器端口。默认值：27000。

c) 单击 **Get Licenses**（获取许可证）。

8. 在“分配许可证”窗口中，指定所需的实例和带宽，然后单击“分配”。



在“管理许可证”页面上，您可以查看许可证服务器、许可证版本以及池中分配的实例和带宽的详细信息。



> 注意
>
> 将永久许可证升级到池化容量不需要重新启动 SDX 设备。

Flexed 或 Pooled 许可证到期和连接问题行为的场景

January 29, 2024

本文档介绍了 NetScaler MPX、NetScaler SDX 和 NetScaler VPX/NetScaler BLX/NetScaler CPX 中许可到期和连接问题行为的不同场景。

灵活许可证的类型

- 软件实例（VPX/BLX/CPX、SDX、MPX、VPX FIPS）
- 带宽容量

MPX FIPS 使用 MPX 软件池中的许可证。SDX FIPS 使用 SDX 软件池中的许可证。VPX FIPS 使用 VPX FIPS 软件池中的许可证。

场景：**MPX** 外形规格

您正在使用灵活/池化许可，许可证即将过期。以下场景说明了在期限到期之前和之后将新许可上载到 NetScaler Console，或者许可文件不存在时的行为。

在任期届满之前

如果在期限到期之前上载了新许可证，并且旧许可证仍然有效，则有两个不同的容量池（新旧容量）可用。

- 如果 NetScaler 已启动并运行，它将在旧许可到期后无缝切换到新的 Flexed/Pooled 许可。
- 不需要重新启动。
- NetScaler 不需要手动重新配置容量。

任期届满后

在这种情况下，现有容量池已过期。

- 在重新启动之前，NetScaler 会一直使用许可运行。
- 如果 NetScaler 重新启动且不存在有效许可文件，则它将变为未经许可。
- 如果 NetScaler 不停地领取新许可，则必须手动对其进行重新配置（重新分配容量）。

场景：**SDX** 外形规格

您正在使用灵活/池化许可，许可证即将过期。以下场景说明了在期限到期之前和之后将新许可上载到 NetScaler Console，或者许可文件不存在时的行为。

在任期届满之前

如果在期限到期之前上载了新许可证，并且旧许可证仍然有效，则有两个不同的容量池（新旧容量）可用。

- 如果 NetScaler 已启动并运行，它将在旧许可到期后无缝切换到新的 Flexed/Pooled 许可。
- 不需要重新启动。
- NetScaler 不需要手动重新配置容量。

任期届满后

在这种情况下，现有容量池已过期。

- 在重新启动之前，NetScaler 会一直使用许可运行。
- 如果管理服务重新启动且不存在有效的许可证文件，则所有 VPX 的吞吐量将降低到 1 Mbps。
- 如果管理服务可以继续领取新许可证，则必须手动对其进行重新配置（重新分配容量）。

场景：**VPX/BLX/CPX** 外形规格

您正在使用灵活/池化许可，许可证即将过期。以下场景说明了在期限到期之前和之后将新许可上载到 NetScaler Console，或者许可文件不存在时的行为。

在任期届满之前

如果在期限到期之前上载了新许可证，并且旧许可证仍然有效，则有两个不同的容量池（新旧容量）可用。

- 如果 NetScaler 已启动并运行，它将在旧许可到期后无缝切换到新的 Flexed/Pooled 许可。
- 不需要重新启动。
- NetScaler 不需要手动重新配置容量。

任期届满后

在这种情况下，现有容量池已过期。

- 在重新启动之前，NetScaler 会一直使用许可运行。
- 如果 NetScaler 重新启动且不存在有效许可文件，则 VPX 和 BLX 将变为未经许可，CPX 变成 CPX Express。
- 如果 NetScaler 不停地领取新许可，则必须手动对其进行重新配置（重新分配容量）。

总结

下表汇总了未在 NetScaler 控制台上应用新许可时所有 NetScaler 外形规格的行为：

外形规格	许可证到期后	在 NetScaler 重启之后
VPX/BLX	一直运行直到重启	VPX/BLX 未获得许可
CPX	一直运行直到重启	CPX 变成 CPX Express
MPX	一直运行直到重启	MPX 变得未获得许可
SDX	一直运行直到重启	所有 VPX 的吞吐量都降低到 1 Mbps（使其无法使用）

连接问题行为的场景

如果 NetScaler 和代理之间或者代理与 NetScaler 控制台服务之间的连接中断，则行为如下所示：

- NetScaler 的宽限期为 30 天。
- 在此宽限期内，许可功能将持续到第三十天。
- 在第三十一天，
  - NetScaler VPX/NetScaler CPX/NetScaler BLX 和 NetScaler MPX 被强制重启并变为未获得许可。
  - NetScaler SDX 上所有 VPX 的吞吐量都降低到 1 Mbps。

仅将 **NetScaler** 控制台服务器配置为 **Flexed** 或 **Pooled** 许可服务器

January 29, 2024

作为管理员，您只能为池化许可功能配置 NetScaler 控制台。使用此配置，NetScaler 控制台仅接收来自 NetScaler 实例的许可数据。

有时，您的监管规定可能要求限制 NetScaler 实例的数据离开监管区域。在这种情况下，您可以在监管区域部署 NetScaler 控制台服务器的本地实例以使用管理、监视和分析功能。当您采用相同的方法使用池化许可功能时，必须将池化许可拆分到各个 NetScaler 控制台许可服务器上。这种方法无法让您灵活地在全球部署的 NetScaler 实例上分配池许可。

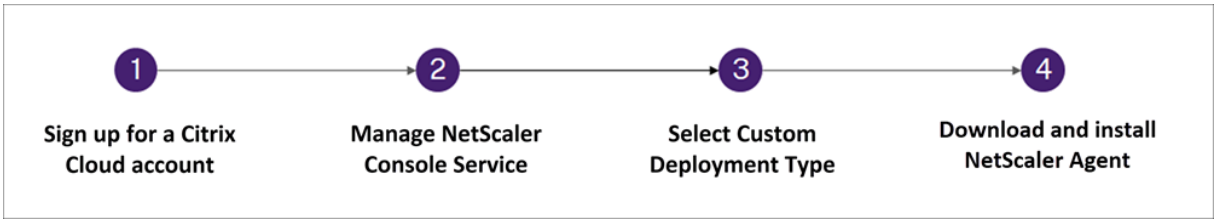
因此，仅为池化许可功能配置 NetScaler 控制台。NetScaler 控制台仅接收来自所有 NetScaler 实例的许可数据。因此，您可以遵守监管规定，在全球部署的 NetScaler 实例上动态分配池容量许可证。

本文档介绍如何仅为池化许可功能配置 NetScaler 控制台。

必备条件

在仅为池化许可功能配置 NetScaler 控制台之前，请先完成 NetScaler 控制台的首次入门和设置。确保查看“系统要求”中的代理规范。

> 重要事项
>
> 当您首次启动或设置 NetScaler 控制台时，请确保以下几点：
>
> - 自定义部署选项处于选中状态。
> - NetScaler 实例将在您完成此配置过程中的步骤 4 后添加



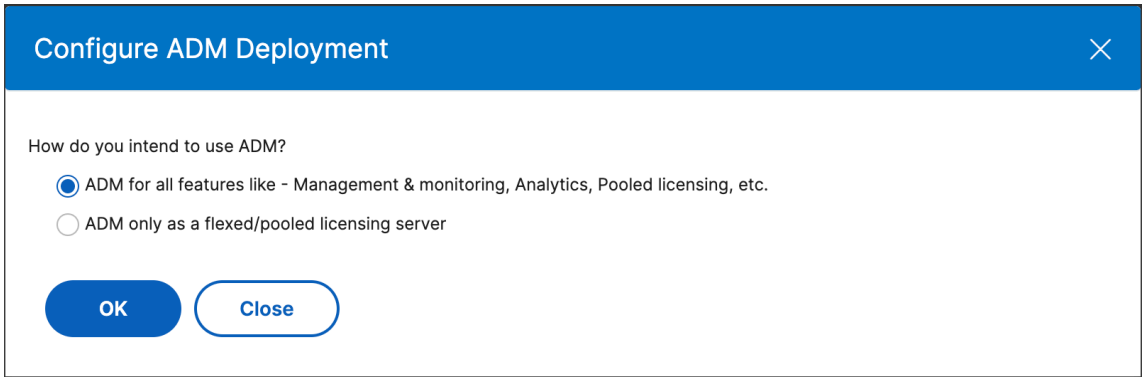
有关入门和设置 NetScaler 控制台的更多信息，请参见入门。

完成入门步骤后，仅为池化许可功能配置 NetScaler 控制台。

如何将 **NetScaler** 控制台仅配置为 **Flexed** 或 **Pooled** 许可服务器

要仅为许可功能配置 NetScaler 控制台，请执行以下操作：

1. 导航到 设置 **>** 全局设置 **>** 系统配置 **>** 系统部署。
2. 在 **NetScaler** 控制台部署中，选择 **NetScaler** 控制台仅作为灵活/池化许可服务器。



3. 单击确定。

   此操作仅保留池化许可功能并禁用以下 NetScaler 控制台功能：

   - NetScaler 控制台备份
   - 事件管理
   - SSL 证书管理
   - 网络报告
   - 网络功能
   - 配置审核

   > 注
   >
   > 意默认情况下，NetScaler 控制台分析功能处于禁用状态。如果已启用此功能，请务必禁用该功能。

   在确认框中，单击 是。

   NetScaler 控制台 GUI 现在仅显示池化许可功能。而且，剩余的功能不会显示。

4. 在仅为许可功能配置 NetScaler 控制台后，在基础架构 **>** 实例页面中添加 NetScaler 实例。

> 注意
>
> - 您也可以在 NetScaler 控制台和其他 NetScaler 控制台服务器中添加 NetScaler 实例。当您更改此类 NetScaler 实例的密码时，请确保更新发现该实例的所有 NetScaler 控制台服务器上的密码。当 NetScaler 控制台配置为仅使用池化许可功能时，本说明适用。
> - 用户仍然可以在 NetScaler 控制台 GUI 中对禁用的功能进行某些操作。例如，事件轮询和 NetScaler 备份。作为超级管理员，如果要限制此类操作，请使用适当的访问策略禁用其他管理员的用户访问权限。有关更多信息，请参见 在 NetScaler 控制台上配置访问策略。

NetScaler VPX 签入和签出许可

January 29, 2024

您可以按需从 NetScaler 控制台向 NetScaler VPX 实例分配 NetScaler VPX 许可。许可由 NetScaler 控制台存储和管理，该控制台的许可框架可提供可扩展的自动许可配置。配置完毕后，NetScaler VPX 实例可以从 NetScaler 控制台签出许可，或者在实例被移除或销毁时将其许可退回 NetScaler 控制台。

在 **NetScaler** 控制台中安装许可

要在 NetScaler 控制台上安装许可文件，请执行以下操作：

1. 导航到 **NetScaler** 许可 **>** 许可管理。
2. 在“许可证文件”部分中，单击“添加许可证文件”，然后选择以下选项之一：
   - 从本地计算机上载许可证文件：如果本地计算机上已经存在许可证文件，则可以将其上载到控制台。
   - 使用许可访问代码：为您从 Citrix 购买的许可指定许可访问代码。单击“获取许可证”，然后单击“完成”。
3. 单击完成。
   许可文件将添加到 NetScaler 控制台中。

   > 注意在使
   >
   > 用许可证访问代码安装许可证之前，请确保您已连接到互联网。

使用 **NetScaler GUI** 将 **NetScaler VPX** 许可分配给 **NetScaler VPX** 实例

1. 登录 NetScaler VPX 实例并导航到“系统”**>**“许可证”**>**“管理许可证”，单击“添加新许可证”，然后选择“使用远程许可”。
2. 在“服务器 名称**/IP** 地址”字段中输入许可证服务器 的详细信息。

   > 注意：如
   >
   > 果您想通过 NetScaler 控制台管理实例的 NetScaler VPX 许可，请选中“向 **NetScaler MA Service** 注册”复选框并输入 NetScaler 控制台凭 据。

3. 单击继续。
4. 在“分配许可证”窗口中，选择许可证类型。该窗口显示总数和可用的虚拟 CPU 以及可以分配的 CPU。单击 **Get Licenses**（获取许可证）。
5. 在下一页上单击“重新启动”以申请许可证。

   > 注意
   >
   > 您还可以释放当前许可证并从其他版本签出。例如，您已经在实例上运行标准版许可证。您可以释放该许可证，然后从高级版中签出。

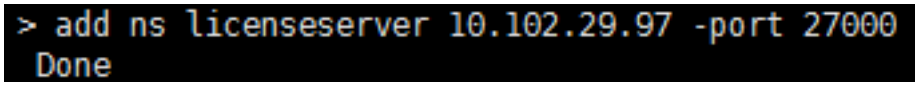
6. 您可以通过导航到“系统”**>**“许可证”**>**“管理许可证”，然后选择“更改分配”或“释放分配”来更改或释放许可证分配。

7. 如果单击 更改分配”，弹出窗口将显示许可证服务器上可用的许可证。选择所需的许可证，单击 获取许可证。

使用 **NetScaler CLI** 向 **NetScaler VPX** 实例分配 **NetScaler VPX** 许可

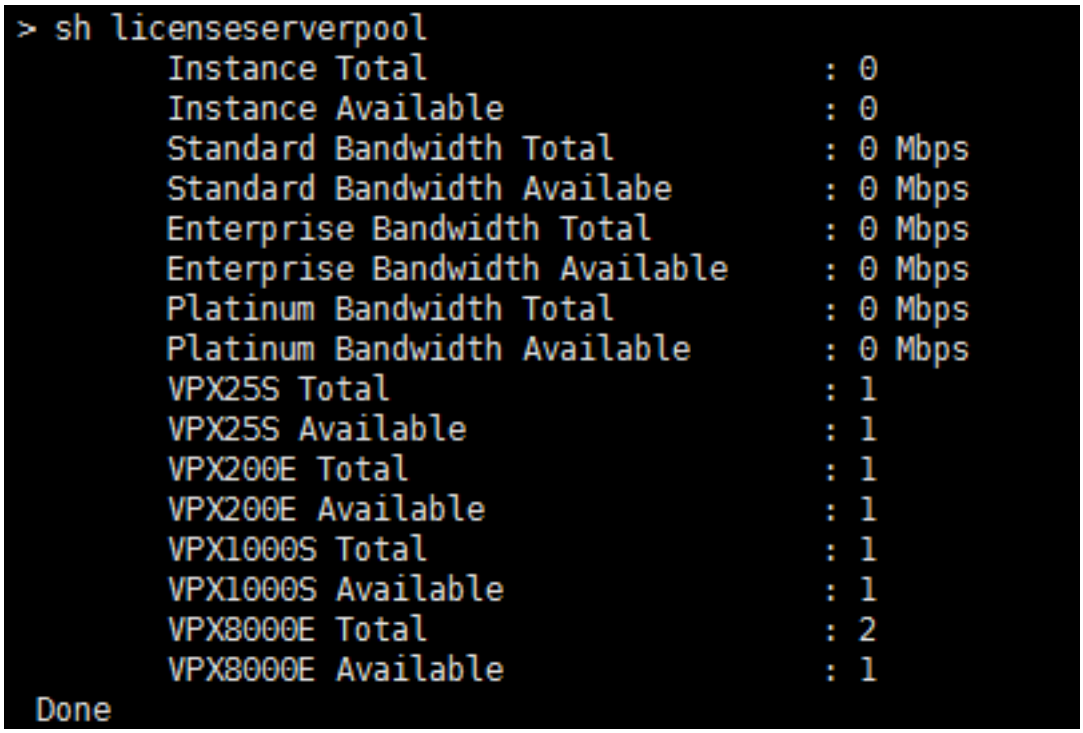
1. 在 SSH 客户端中，输入 NetScaler 实例的 IP 地址，然后使用管理员凭据登录。
2. 要添加许可服务器，请输入以下命令：

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
```



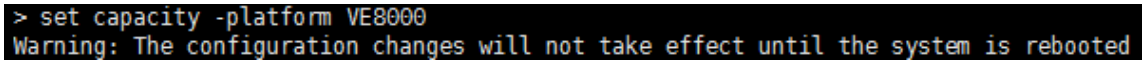
3. 要显示许可服务器上的可用许可证，请输入以下命令：

```
sh licenseserverpool
```



4. 要为 NetScaler VPX 实例分配许可，请输入以下命令：

```
set capacity  - platform V[S/E/P][Bandwidth]
```



为 **NetScaler VPX** 签入/签出许可证配置到期检查

现在，您可以为 NetScaler VPX 许可配置许可到期阈值。通过设置阈值，NetScaler 控制台会在许可到期时通过电子邮件或短信发送通知。当许可在 NetScaler 控制台上过期时，还会发送 SNMP 陷阱和通知。

发送许可到期通知时会生成一个事件，可以在 NetScaler 控制台上查看此事件。

有关更多信息，请参阅 许可证管理。

NetScaler 虚拟 **CPU** 许可

January 29, 2024

像您这样的数据中心管理员正在转向更新的技术，这些技术可以简化网络功能，同时提供更低的成本和更大的可扩展性。较新的数据中心架构必须至少包含以下功能：

- 软件定义网络 (SDN)
- 网络功能虚拟化 (NFV)
- 网络虚拟化 (NV)
- 微型服务

这种运动还需要软件要求动态、灵活和敏捷，以满足不断变化的业务需求。许可证还将由一个中央管理工具管理，并充分了解使用情况。

NetScaler VPX 的虚拟 **CPU** 许可

早些时候，NetScaler VPX 许可证是根据实例的带宽消耗分配的。NetScaler VPX 仅限使用基于其绑定许可证版本的特定带宽和其他性能指标。要增加可用带宽，必须升级到提供更多带宽的许可证版本。在某些情况下，带宽要求可能较低，但对其他 L7 性能（例如 SSL TPS、压缩吞吐量等）的要求更高。在这种情况下，升级 NetScaler VPX 许可证可能不合适。但是，您可能仍然需要购买带宽较大的许可证，以解锁 CPU 密集处理所需的系统资源。NetScaler 控制台现在支持根据虚拟 CPU 要求向 NetScaler 实例分配许可证。

在基于 CPU 使用情况的虚拟许可功能中，许可证指定特定 NetScaler VPX 有权使用的 CPU 数量。因此，NetScaler VPX 只能从许可证服务器检出其上运行的虚拟 CPU 数量的许可证。NetScaler VPX 会根据系统中运行的 CPU 数量签出许可证。NetScaler VPX 在签出许可证时不考虑空闲 CPU。
与池化许可容量和 CICO 许可功能类似，NetScaler 控制台许可服务器管理一组单独的虚拟 CPU 许可。此外，管理虚拟 CPU 许可证的三个版本是标准版、高级版和高级版。这些版本解锁了与带宽许可证版本解锁的功能集相同。

虚拟 CPU 的数量可能会发生变化，或者许可证版本有变化时。在这种情况下，您必须始终关闭实例，然后再发起新许可证集的请求。签出许可证后重新启动 NetScaler VPX。

使用 **GUI** 在 **NetScaler VPX** 中配置许可服务器

1. 在 NetScaler VPX 中，导航到“系统”>“许可证”，然后单击“管理许可证”。
2. 在“许可证”页面上，单击“添加新许可证”。
3. 在“许可证”页面上，选择“使用远程许可”选项。
4. 从“远程许可模式”列表中选择 CPU 许可。
5. 键入许可证服务器的 IP 地址和端口号。
6. 单击继续。

   > 注
   >
   > 意：请务必在 NetScaler 控制台中注册 NetScaler VPX 实例。如果尚未完成，请启用“向 NetScaler 控制台注册”，然后键入 NetScaler 控制台登录凭据。

7. 在“分配许可证”窗口中，选择许可证类型。该窗口显示总数和可用的虚拟 CPU 以及可以分配的 CPU。单击 **Get Licenses**（获取许可证）。

   > 注
   >
   > 意：对于 NetScaler HA 对，请分别为每个节点分配虚拟 CPU 许可证。

8. 单击下一页上的 重新启动 以申请许可证。

   > 注意
   >
   > 您还可以释放当前许可证并从其他版本签出。例如，您已经在实例上运行标准版许可证。您可以释放该许可证，然后从高级版中退出。

常见问题解答和其他资源

April 10, 2024

本节列出了有关配置和操作池化许可的参考文档。您可以参阅这些文档以获取与配置和操作问题相关的帮助。

配置

1. 在哪里可以找到有关池化容量的概述和功能的信息？

   答案：请参阅 配置池化容量。

2. 如何将永久许可证转换或迁移到池化许可证，反之亦然？

   答：从永久许可证转换为池化容量许可证是一个单向许可授权过程。您无法将池容量许可证恢复为永久许可证。

3. 如何部署 NetScaler 控制台服务器?

   回答：按照入门文档进行操作。

4. 如何向现有的池化许可证添加许可证并进行分配?

   答：遵循许可证管理文档。

5. 如何在实例上分配/增加容量和带宽?

   答：遵循许可证管理文档。

许可证服务器代理

1. 如何将 LSA 角色分配给特定代理?

   答案：部署的第一个代理被分配了 LSA 角色。如果 LSA 代理出现故障，所有连接到 NetScaler 控制台进行池化许可的 NetScaler 实例将进入为期一天的宽限期。第二天，NetScaler 控制台选择了一个新的代理作为 LSA。默认情况下，此行为处于启用状态。

   管理员可以在 24 小时内手动选择 NetScaler 代理作为 LSA，而不必等待 NetScaler 控制台服务在 LSA 关闭 24 小时后自动选择代理。

   > 注意：
   >
   > 在此过渡期间，NetScaler 功能不受影响。

2. 我们如何确定哪个代理托管许可证服务器角色?

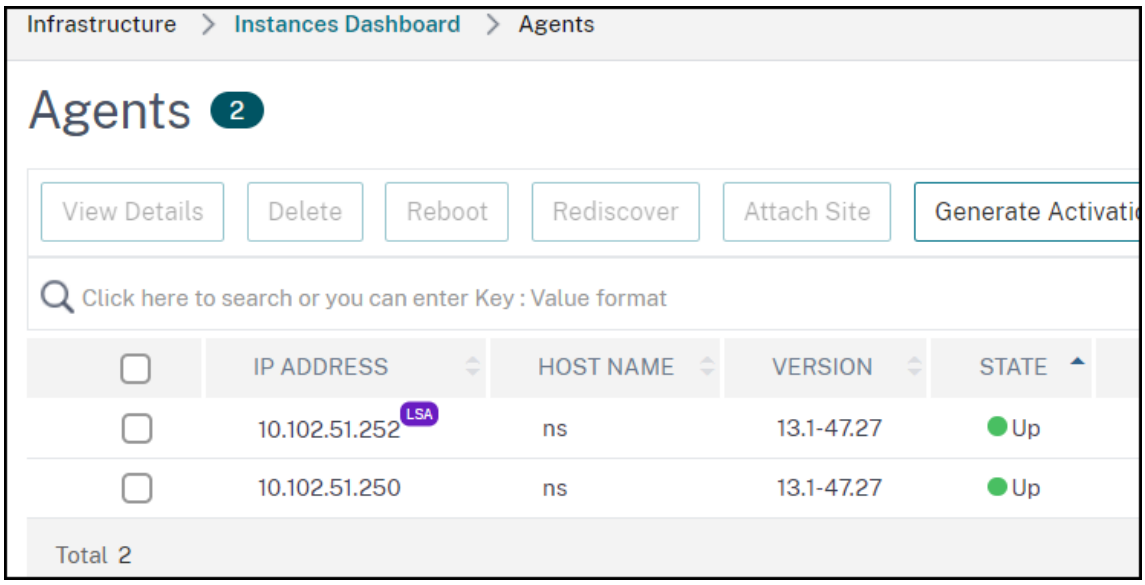
   答：要知道哪个代理托管 LSA 角色，可以在 shell 中运行以下命令：

   ```
   cat /mpsconfig/.lmp/agent
   ```

   如果“角色”的输出值为 **lsa**，则该代理托管许可证服务器角色。

   在 NetScaler 控制台 GUI 中，您会看到 LSA 写在指定代理的 IP 地址旁边。



3. 当托管 LSA 角色的代理出现故障时会发生什么？

   答：如果托管 LSA 角色的代理处于脱机状态，则为池化容量许可配置的所有已部署的 NetScaler 设备都将进入宽限期。宽限期持续 30 天，分配给 NetScaler 设备的资源将持续到此期间。在此状态下的 NetScaler 实例在托管 LSA 角色的代理再次联机或指定具有 LSA 角色的新代理之前，无法分配或修改许可分配。

4. 如果担任 LSA 角色的代理长时间处于脱机状态，会连任吗？

   答：如果管理员未在 24 小时内选择新的 LSA，则在 LSA 代理关闭 24 小时后，NetScaler 控制台服务会自动选择下一个启动的代理作为新的 LSA。当选新 LSA 后，NetScaler 设备的宽限期结束。

常见问题

1. 由于连接故障、升级、大脑分裂等原因，实例在宽限模式下运行。

   答：参见 配置 NetScaler 池容量中记录的 NetScaler 控制台许可服务器行为。

2. 许可证未应用或反映实例。

   答案：请参见 池容量许可证问题故障排除。

3. 许可证分配陷入“同步进行中”。

   答案：请参见 池容量许可证问题故障排除。

4. 由于许可证文件上的主机 ID 错误而出错。

   答：要识别 NetScaler 控制台服务器，可以为该服务器分配主机名。主机名显示在 NetScaler 控制台的通用许可上。有关详细信息，请参见 为 NetScaler 控制台服务器分配主机名。

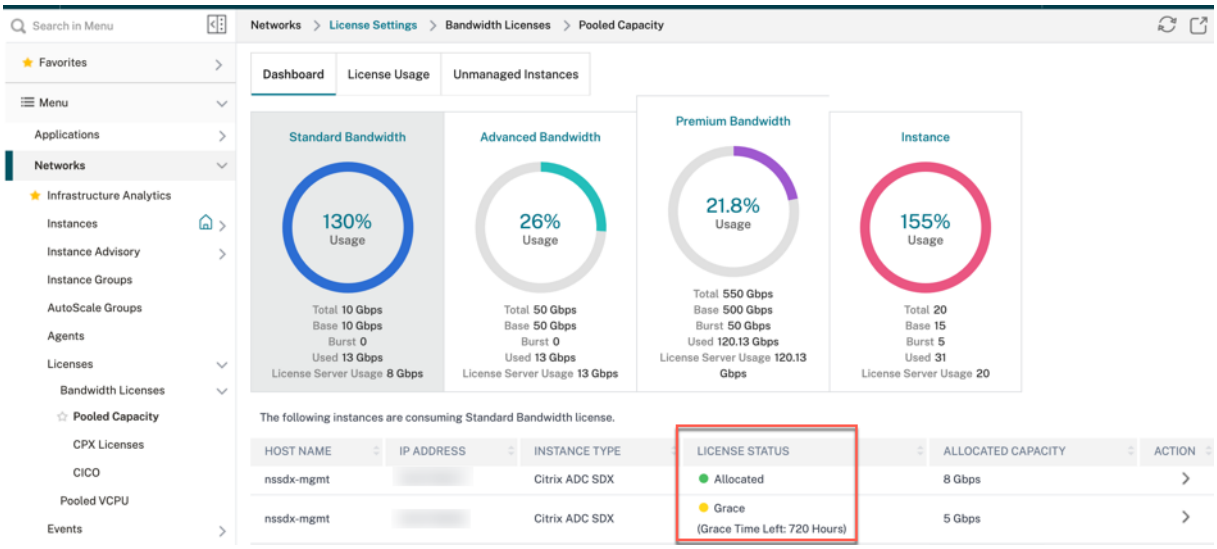
对池容量许可证问题进行故障排除

January 29, 2024

本节介绍如何分析和解决常见的池化容量问题。

查看许可证状态

NetScaler 控制台充当您的 NetScaler 池容量许可的许可服务器。您可以使用 NetScaler 控制台 GUI 来检查许可状态。导航到 基础结构 **>** 池化许可 **>** 池容量 **>** 许可证使用情况。



下表列出了许可证状态的类型及其含义

状态	这意味着什么
已分配	许可证状态没问题。
已分配：未应用于 NetScaler	如果从 NetScaler 签出或签入许可，NetScaler 可能需要重启，但是 NetScaler 尚未重启。
未分配	未在 NetScaler 实例中分配许可。
格蕾丝	NetScaler 实例在许可证宽限期内为 30 天
正在同步	NetScaler 控制台以 2 分钟为间隔从 NetScaler 获取信息。在 NetScaler 控制台和 NetScaler 之间同步许可可能需要长达 15 分钟。NetScaler 控制台可能已重新启动或触发了 NetScaler 控制台的故障转移。

状态	这意味着什么
部分拨款项	NetScaler 无法接受分配的容量，因为它可能在最大分配的情况下运行。例如，NetScaler 运行时的许可证池容量为 10 Gbps。当 NetScaler 重新启动时，10 Gbps 将签回 NetScaler 控制台许可服务器。当 NetScaler 重新联机时，它会尝试自动检出之前分配的 10 Gbps。同时，其他 NetScaler 实例可能已经检查了该带宽。如果许可池没有足够的容量为此 NetScaler 分配完整 10 Gbps 甚至部分容量，则会显示“已部分分配”。
不受管理	出于可管理性考虑，没有将 NetScaler 添加到 NetScaler 控制台中。这不会对 NetScaler 许可产生影响，但会影响 NetScaler 控制台的许可监视。
不受管理	出于可管理性考虑，没有将 NetScaler 添加到 NetScaler 控制台中。这不会对 NetScaler 许可产生影响，但会影响 NetScaler 控制台的许可监视。
连接已断开	出于可管理性考虑，无法从 NetScaler 控制台访问 NetScaler。例如，存在网络连接问题、NITRO 无法正常工作或 NetScaler 密码不匹配。如果 NITRO 无法正常工作或 NetScaler 密码不匹配，则不会影响 NetScaler 许可。但是，它可能会影响 NetScaler 控制台的许可监视。

检查服务器状态

本节介绍常见的服务器状态问题以及可能的原因和修复方法。

问题：NetScaler 将许可服务器显示为无法访问，许可状态更改为宽限。

- 与许可服务器（NetScaler 控制台或代理）的连接已中断超过 15 分钟。验证许可证服务器是否已启动并可访问。
- NetScaler 处于宽限模式。

问题：NetScaler 将许可服务器状态显示为可访问，但用户尝试更改分配无效。单击“更改分配”返回 0 0。此值可能会使配置的容量看起来已丢失。

- 与许可服务器的连接最近出现故障，但是 NetScaler 仍未错过第二次心跳。因此，它不在格雷斯中（还）。验证许可证服务器是否已启动并可访问。

问题：NetScaler 显示容量和实例数，但许可服务器处于可访问/无法访问状态。单击“更改分配”将返回一些数字，但不考虑配置的容量。

- 与许可服务器的连接已恢复，但是 NetScaler 仍无法错过第二次心跳或发送重新连接探测器。

问题：NetScaler 说，使用 NetScaler 控制台配置池化许可时无法连接到许可服务器

- 检查防火墙规则，确保端口 27000 和 7279 处于打开状态。
- 该代理未注册。有关更多信息，请参阅 入门。
- NetScaler 控制台没有上载许可文件。有关详细信息，请参见 配置 NetScaler 池容量
- NetScaler 控制台的许可文件错误。

查看许可证的使用报告

在 **NetScaler** 控制台 **GUI** 中的 **NetScaler** 许可 **>** 池化许可 **>** 带宽许可 **>** 池化容量 > 许可使用情况 下，您可以看到许可使用量的每月峰值。您可以使用此报告来增加许可证使用量或计划购买额外的许可证。

以下是如何生成和使用报告的一些详细信息。

轮询：每 15 分钟从 NetScaler 实例轮询一次许可数据。

保持每小时峰值：NetScaler 控制台仅维持每台设备一小时内的最大许可使用量。

报告：您可以为特定时间范围内的每个实例生成 GUI 报告。

导出：您可以以 CSV 格式或 XLS 格式导出报告。

清除：NetScaler 控制台会在每月第一天凌晨 12:10 清除数据。清除周期是可配置的（默认时段为两个月）。

池化容量许可的计数器和统计信息

以下计数器、日志和命令暴露了 NetScaler 池许可指标，这些指标表明 NetScaler 控制台和 NetScaler 实例在池化许可模式下的行为。

- **SNMP** 陷阱：从 NetScaler 版本 13.xx 中可用。
- **NSCONMSG** 限速 计数器：从 NetScaler 版本 12.1 57.xx 中可用。
- **NetScaler** 控制台计数器 NetSc aler 控制台命令操作在 NetScaler 云服务中可用。

SNMP 陷阱

您可以配置以下 SNMP 陷阱 v.13 池化许可证警报

- `POOLED-LICENSE-CHECKOUT-FAILURE`
- `POOLED-LICENSE-ONGRACE`
- `Configure POOLED-LICENSE-PARTIAL`

有关这些警报的更多信息，请参阅 NetScaler SNMP OID 参考。

NSCONMSG 计数器

检查以下 NCCONMSG 计数器及其含义：

- allnic_err_rl_cpu_pkt_drops：达到 CPU 限制后聚合（所有 NIC）数据包丢弃
- allnic_err_rl_pps_pkt_drops：在 pps 限制之后，整个系统内的数据包丢弃
- allnic_err_rl_rate_pkt_drops：整个系统内的总利率下降
- allnic_err_rl_pkt_drops：由于速率、点数和 CPU 导致的累计速率限制下降
- rl_tot_ssl_rl_enforced：SSL RL 的应用次数（在新的 SSL 连接上）
- rl_tot_ssl_rl_data_limited: 达到 SSL 吞吐量限制的次数
- rl_tot_ssl_rl_sess_limited: 达到 SSL TPS 限制的次数

NetScaler 控制台计数器

选择“运行命令操作”事件操作 时，您可以为符合特定筛选条件的事件创建命令或脚本，该命令或脚本可在 NetScaler 控制台上运行。
您还可以为 运行命令操作 脚本设置以下参数：

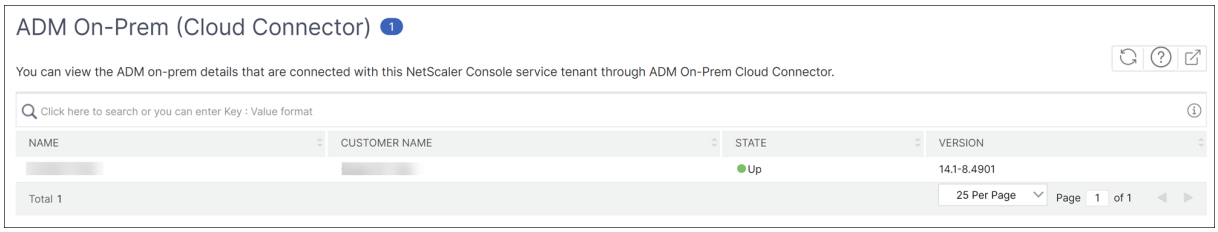
参数	说明
$source	此参数对应于接收的事件的源 IP 地址。
$category	此参数对应于筛选器类别下定义的陷阱类型。
$entity	此参数对应于已为其生成事件的实体实例或计数器。它可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、所有证书相关事件的证书名称。
$severity	此参数对应于事件的严重性。
$failureobj	故障对象会影响事件的处理方式，并确保故障对象反映所通知的确切问题。此参数可用于快速追踪问题和确定失败原因，而不仅仅是报告原始事件。

> 注意
>
> 在命令执行过程中，这些参数将替换为实际值。

使用 Cloud Connect 与控制台服务连接的控制台本地实例

March 10, 2024

在设置 **> NetScaler** 控制台本地部署中，您可以查看通过 Cloud Connect 与控制台服务租户连接的控制台本地实例的详细信息。



- 名称 -本地 NetScaler 控制台的 IP 地址
- 客户名称 -NetScaler 控制台服务租户的名称
- 状态 - NetScaler 控制台本地实例与 NetScaler 控制台服务之间的连接状态
- 版本 - NetScaler 控制台本地实例构建版本

主机本地上载

July 17, 2024

此页面仅适用于选择手动模式将其遥测数据上载到 NetScaler 控制台服务的 NetScaler 本地用户。确保您已从本地的 NetScaler 控制台下载了遥测数据（单击 **NetScaler** 遥测主页上的下载遥测数据，下载包含所需遥测数据的捆绑包 (.tgz) 文件）。

要在 NetScaler 控制台服务中上载您的数据遥测数据，请执行以下操作：

1. 在 **NetScaler** 控制台本地上载页面中，单击“上载遥测”，然后选择下载的 (.tgz) 文件以完成上载过程。
2. 在选择手动模式后 30 天内完成首次上载。重复相同的程序，此后每隔 90 天上载遥测文件。

> 备注：
>
> - 如果文件不是有效的 (.tgz) 格式或者文件未通过完整性检查，则上载将失败。建议重新下载并重试上载。如果问题仍然存在，请联系客户服务。
> - 您可以禁用可选的遥测数据。要禁用，在 NetScaler 控制台本地环境中，必须先在 **NetScaler** 遥测页面中禁用“安全公告”，然后导航到“设置”**>**“管理”**>**“启用或禁用 **Console** 功能数据共享”，并清除“我同意共享控制台功能使用数据”复选框。

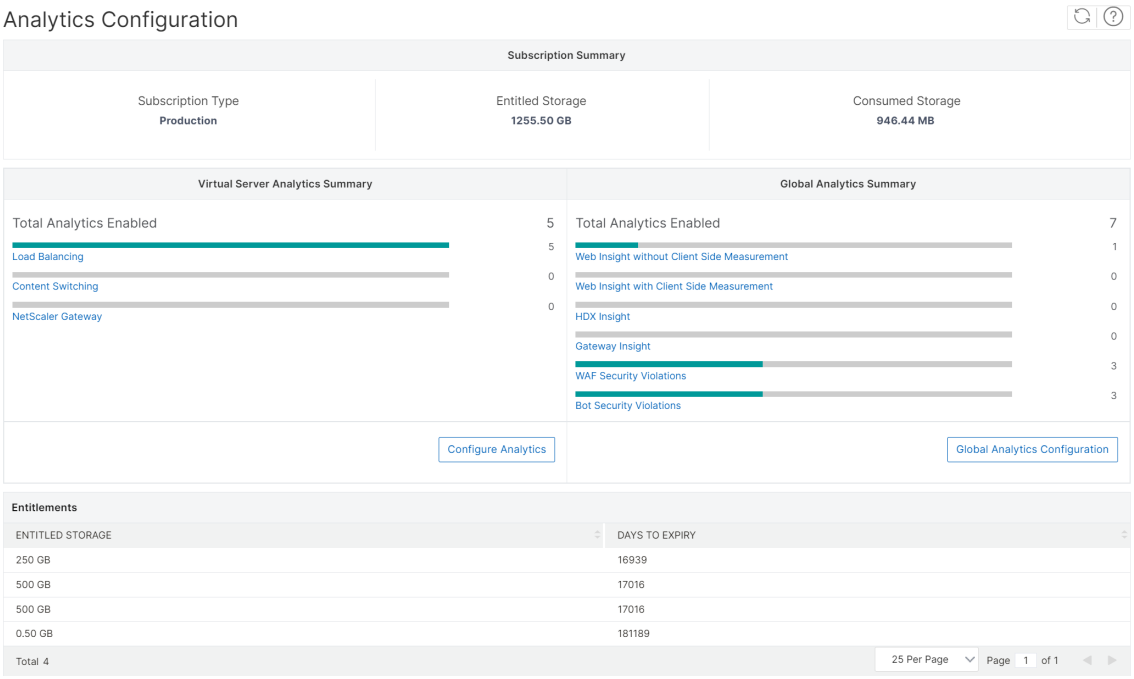
在虚拟服务器上配置分析

March 10, 2024

从 14.1-21.x 版本开始，所有发现的虚拟服务器和后续虚拟服务器都将自动获得许可。您可以继续配置分析。

您可以通过两种方式配置分析。导航到“设置”**>**“分析配置”以查看：

- 虚拟服务器分析摘要 -使您能够在发现的虚拟服务器上配置分析。
- 全局分析摘要 -使您能够在已发现的和后续的虚拟服务器上配置分析。



在发现的虚拟服务器上配置分析

> 注意：
>
> 确保要启用分析的虚拟服务器处于 **UP** 状态。

1. 在“虚拟服务器分析摘要”下，单击“配置分析”。

   此时将显示 所有虚拟服务器 页面。您可以：

   - 启用分析
   - 编辑分析
   - 禁用分析

   > 注意：
   >
   > 支持用于启用分析的虚拟服务器是负载平衡、内容切换和 NetScaler Gateway。

2. 选择虚拟服务器，然后单击“启用安全和分析”。

> 注意
>
> 或者，您可以为实例启用分析：
>
> ```
> 1. 导航到 **基础结构 > 实例 > NetScaler** ，然后选择实例类型。例如，VPX。
> 2
> 3 1. 选择实例，然后从“**选**择操作”列表中选择“配置分**析**”
> 4 1. 在“**在虚拟服务器上配置分析**”页面上，选择虚拟服务器，然后单击“**启用安全与分析**”。
> ```

3. 在“启用安全与分析”窗口中：

   a) 选择洞察类型。

   b) 选择 **Logstream** 作为传输模式。

   > 注意：
   >
   > 对于 NetScaler 12.0 或更低版本，**IPFIX** 是传输模式的默认选项。对于 NetScaler 12.0 或更高版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。
   >
   > 有关 IPFIX 和 Logstream 的更多信息，请参阅 Logstream 概述。

   c) 在 实例级别选项下：

   - 启用 **HTTP X-Forwarded-For** -选择此选项可标识客户端和应用程序之间通过 HTTP 代理或负载平衡器进行连接的 IP 地址。
   - **NetScaler Gateway** -选择此选项可查看 NetScaler Gateway 的分析。

   d) 默认情况下，表达式为真。

   e) 单击确定。

   > 注意：
   >
   > - 对于管理分区，仅支持 **Web Insight** 。
   > - 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。将显示一条错误消息。

单击“确定”后，NetScaler 控制台将处理以启用对所选虚拟服务器的分析。

> 注意
>
> NetScaler 控制台使用 NetScaler SNIP 作为 Logstream，使用 NSIP 进行 IPFIX。如果在 NetScaler 代理和 NetScaler 实例之间启用了防火墙，请确保打开以下端口，以使 NetScaler 控制台能够收集 AppFlow 流量：

传输模式	源 IP	类型	端口
IPFIX	NSIP	UDP	4739
Logstream	SNIP	TCP	5557

编辑分析

要编辑虚拟服务器上的分析，请执行以下操作：

1. 选择虚拟服务器。

   > 注意：
   >
   > 或者，您也可以编辑实例的分析：
   >
   > ```
   > 1. 导航到 **基础结构 > 实例 > NetScaler** ，然后选择实例类型。例如，VPX。
   > 2.
   > 3. 选择实例，然后单击“**编辑安全和分析**”。
   > ```

2. 单击“编辑安全与分析”
3. 在“编辑 分析配置”窗口中编辑 要应用的参数。
4. 单击确定。

禁用分析

要在选定的虚拟服务器上禁用分析，请执行以下操作：

1. 选择虚拟服务器。
2. 单击“禁用分析”。

NetScaler 控制台禁用对所选虚拟服务器的分析。

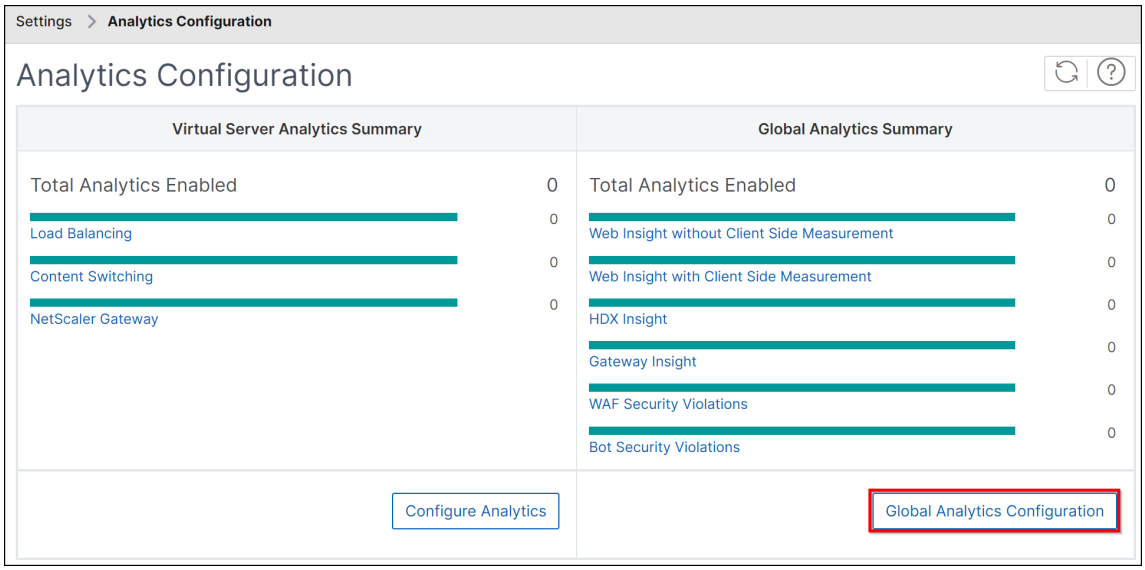
下表描述了支持 IPFIX 和 Logstream 作为传输模式的 NetScaler 控制台的功能：

功能	IPFIX	Logstream
Web Insight	•	•
WAF 安全违规	•	•
Gateway Insight	•	•
HDX Insight	•	•

功能	IPFIX	Logstream
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

全局配置分析

1. 在“全局分析摘要”下，单击“全局分析配置”。



2. 选择要在虚拟服务器上启用分析的分析功能。
3. 单击 Submit（提交）。

配置完成后，将在已发现的和后续的虚拟服务器上启用分析。

需要注意的事项

- 假设您是通过选择 **Web Insight**、**HDX Insight** 和 **Gateway Insight** 首次配置全局分析配置。如果您稍后再次更改分析设置并取消选择 **Gateway Insight**，则这些更改不会影响已经启用分析功能的虚拟服务器。
- 假设您有 10 个虚拟服务器，其中两台已经使用“配置分析”选项启用了分析。在这种情况下，当您配置全局分析配置时，分析仅应用于其余八个虚拟服务器。

- 假设您有 10 个虚拟服务器，并且手动禁用了对两台虚拟服务器的分析。在这种情况下，当您配置全局分析配置时，分析仅应用于其余八个虚拟服务器，并且会跳过通过分析手动禁用的虚拟服务器。

配置基于角色的访问控制

March 10, 2024

NetScaler 控制台提供精细的、基于角色的访问控制 (RBAC)，您可以根据企业内个人用户的角色授予访问权限。

在 NetScaler 控制台中，所有用户都添加到 Citrix Cloud 中。作为组织的第一个用户，您必须先在 Citrix Cloud 中创建一个帐户，然后使用 Citrix Cloud 凭据登录 NetScaler 控制台 GUI。您被授予超级管理员角色，默认情况下，您拥有 NetScaler 控制台中的所有访问权限。稍后，您可以在 Citrix Cloud 中在组织中创建其他用户。

稍后创建并以普通用户身份登录到 NetScaler 控制台的用户被称为委托管理员。默认情况下，这些用户拥有除用户管理权限之外的所有权限。但是，您可以通过创建相应的策略并将其分配给这些委派用户来授予特定的用户管理权限。用户管理权限位于“设置”**>**“用户和角色”。

有关如何分配特定权限的更多信息，请参阅 如何向委派管理员用户分配额外权限。

以下各节提供了有关如何创建策略、角色、组以及如何将用户绑定到组的更多信息。

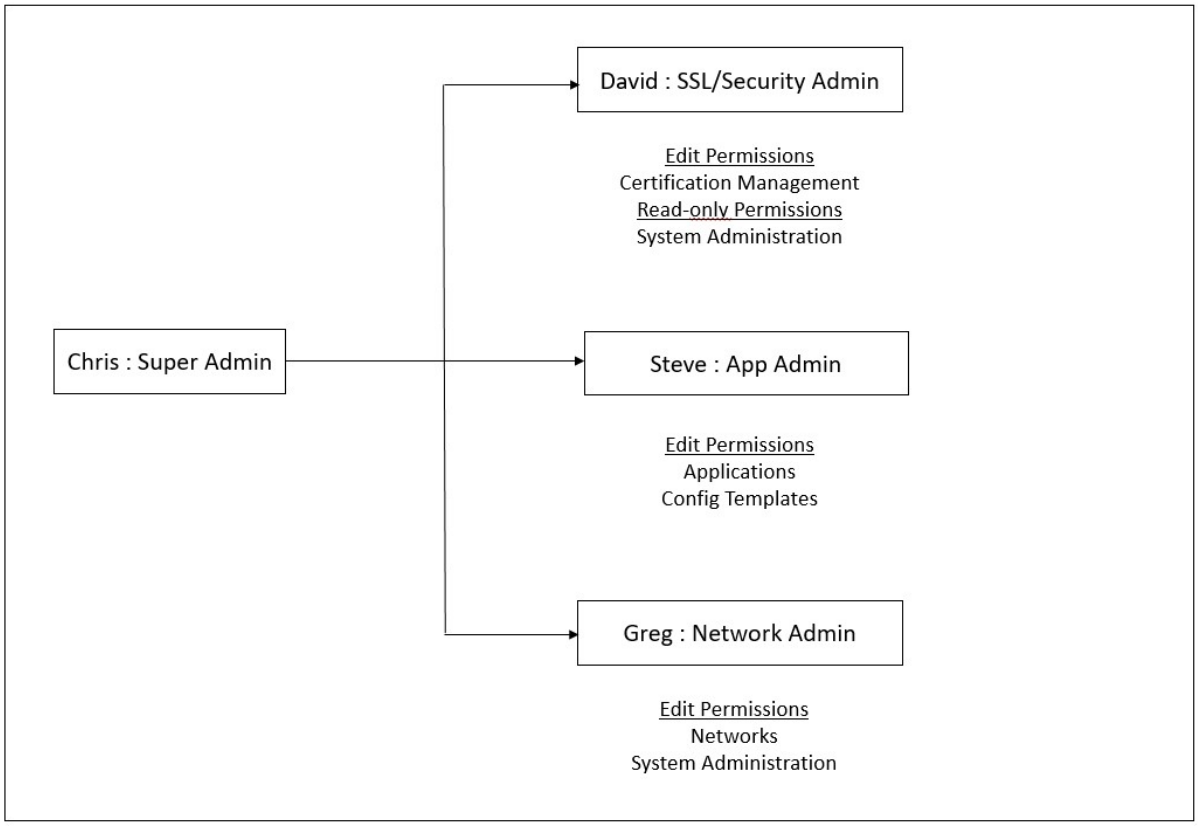
示例：

以下示例说明了如何在 NetScaler 控制台中实现 RBAC。

NetScaler 小组负责人 Chris 是其组织中 NetScaler 控制台的超级管理员。他创建三个管理员角色：安全管理员、应用程序管理员和网络管理员。

- 安全管理员 David 必须具有 SSL 证书管理和监视的完全访问权限，但必须具有系统管理操作的只读访问权限。
- 应用程序管理员 Steve 需要只对特定应用程序和特定配置模板拥有访问权限。
- 网络管理员 Greg 需要访问系统和网络管理的权限。
- Chris 还必须为所有用户提供 RBAC，无论他们是本地还是外部用户。

下图显示了管理员和其他用户拥有的权限以及他们在组织中的角色。



为了向用户提供基于角色的访问控制，Chris 必须先在 Citrix Cloud 中添加用户，之后他才能在 NetScaler 控制台中看到这些用户。Chris 必须根据每个用户的角色为其创建访问策略。访问策略与角色紧密相关。因此，Chris 还必须创建角色，然后他必须创建组，因为角色只能分配给组，不能分配给单个用户。

访问权限是执行特定任务（例如查看、创建、修改或删除文件）的能力。角色是根据企业内用户的权限和责任定义的。例如，可能允许一个用户执行所有网络操作，而另一个用户可以观察应用程序中的流量流量并帮助创建配置模板。

策略决定用户角色。创建策略后，您可以创建角色，将每个角色绑定到一个或多个策略，并将角色分配给用户。您还可以为用户组分配角色。组是拥有共同权限的用户集合。例如，管理特定数据中心的用户可以分配到一个组。角色是通过根据特定条件将用户添加到特定组来授予用户的身份。在 NetScaler 控制台中，创建角色和策略特定于 NetScaler 中的 RBAC 功能。可以根据企业逐步发展的需求轻松地创建、更改或停用角色和策略，而无需单独更新每个用户的权限。

角色可以基于功能，也可以基于资源。例如，假定一个 SSL/安全管理员和一个应用程序管理员。SSL/安全管理员必须对 SSL 证书管理和监视功能具有完全访问权限，但对于系统管理操作必须具有只读访问权限。应用程序管理员只能访问其范围内的资源。

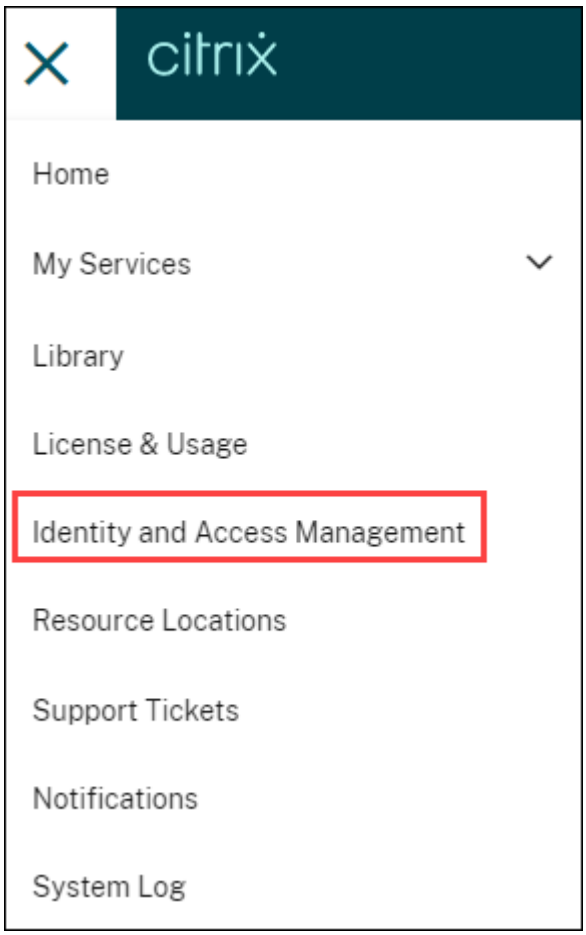
因此，以超级管理员 Chris 的身份在 NetScaler 控制台中执行以下示例任务，为组织中的安全管理员 David 配置访问策略、角色和用户组。

在 **NetScaler** 控制台上配置用户

作为超级管理员，您可以通过在 Citrix Cloud 而不是在 NetScaler 控制台中为他们配置帐户来创建更多用户。将新用户添加到 NetScaler 控制台后，您只能通过向用户分配相应的组来定义他们的权限。

要在 **Citrix Cloud** 中添加新用户，请执行以下操作：

1. 在 NetScaler 控制台 GUI 中，单击左上角的汉堡图标，然后选择身份和访问管理。

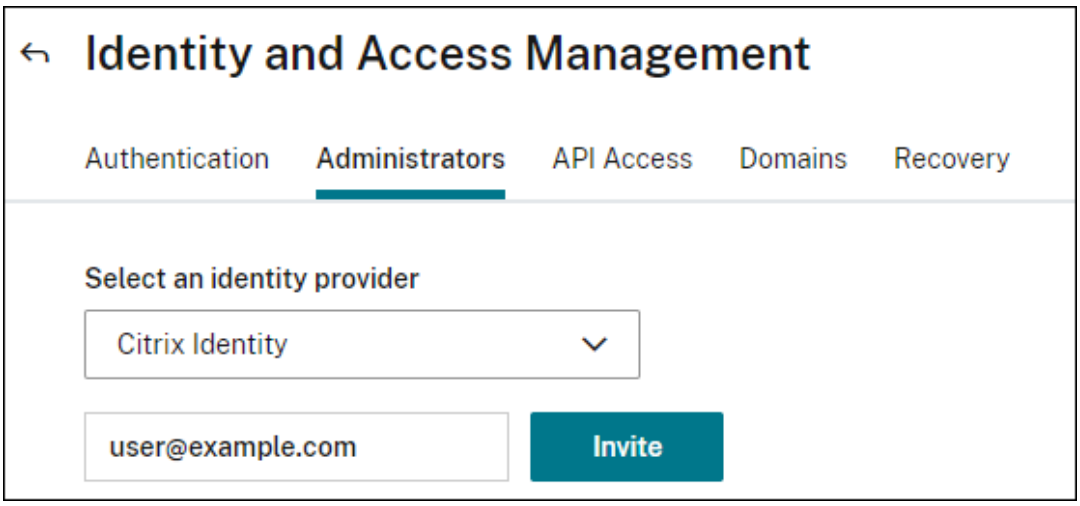


2. 在“身份和访问管理”页面上，选择“管理 员”选项卡。

   此选项卡列出了在 Citrix Cloud 中创建的用户。

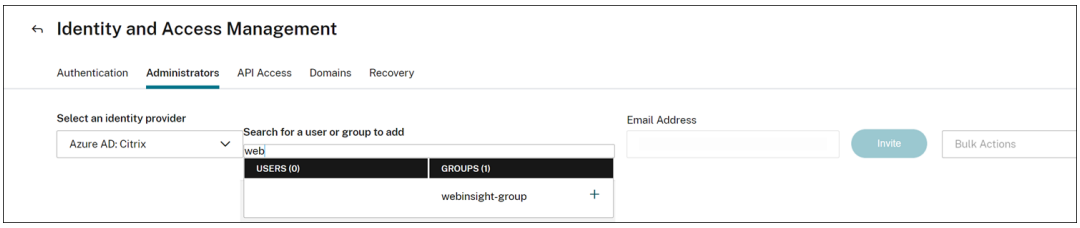
3. 从列表中选择身份提供商。

   - **Citrix** 身份：键入要在 NetScaler 控制台中添加的用户的电子邮件地址，然后单击“邀请”。



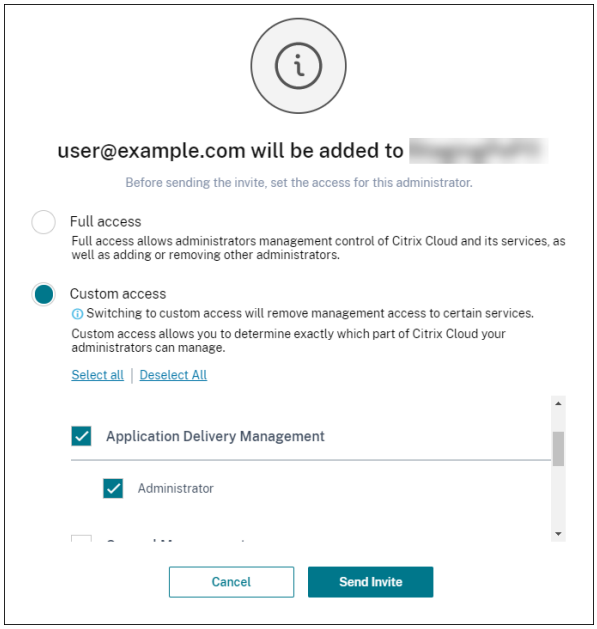
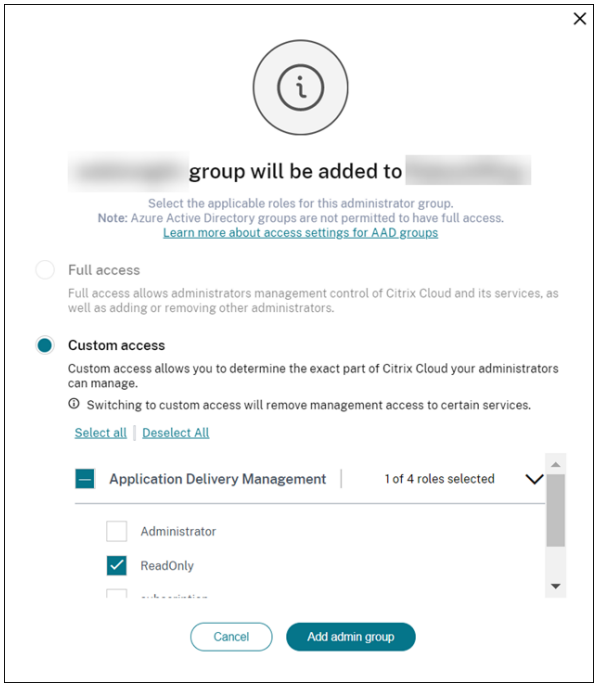
> 注意：
>
> 用户会收到来自 Citrix Cloud 的电子邮件邀请。用户必须单击电子邮件中提供的链接，通过提供其全名和密码完成注册过程，然后使用其凭据登录 NetScaler Console。

- **Azure Active Directory (AD)**：只有当您的 Azure AD 连接到 Citrix Cloud 时，此选项才会出现，请参阅 将 Azure ActiveDirectory 选择此选项邀请用户或组时，只能为选定的用户或组指定“自定义访问权限”。用户可以使用他们的 Azure AD 凭据登录 NetScaler 控制台。而且，您不需要为属于所选 Azure AD 的用户创建 Citrix 身份。如果用户被添加到受邀组，则无需向新添加的用户发送邀请。该用户可以使用 Azure AD 凭据访问 NetScaler 控制台。



4. 为指定用户或组选择“自定义访问权限”。
5. 选择 应用程序交付管理。

   此选项列出了在 NetScaler 控制台中创建的用户组。选择要向其添加用户的组。

Citrix 身份	Azure AD
	
单击发送邀请。	单击“添加管理员组”。

作为管理员，只有在用户登录到 NetScaler 控制台后，您才能在 NetScaler 控制台用户列表中看到新用户。

要在 **NetScaler** 控制台中配置用户，请执行以下操作：

1. 在 NetScaler 控制台 GUI 中，导航 到 设置 > 用户和角色 > 用户。
2. 用户将显示在“用 户 页面上。
3. 您可以通过选择用户并单击“编辑”来 编辑向用户提供的权限。您还可以在“设 置”节点下的“组”页面上编辑群 组权限。

   > 注意：
   >
   > - 用户只能从 Citrix Cloud 添加到 NetScaler 控制台中。因此，即使您拥有管理员权限，也无法在 NetScaler 控制台 GUI 中添加或删除用户。您只能编辑组权限。可以在 Citrix Cloud 中添加或删除用户。
   > - 只有在用户登录到 NetScaler 控制台至少一次后，用户详细信息才会显示在服务 GUI 上。

在 **NetScaler** 控制台上配置访问策略

访问策略定义权限。可以通过创建角色将策略应用于一个用户组或多个组。策略决定用户角色。创建策略后，您必须创建角色，将每个角色绑定到一个或多个策略，并将角色分配给用户组。NetScaler 控制台提供五种预定义的访问策略：

- **admin_polic**y。授予对所有 NetScaler 控制台节点的访问权限。用户拥有查看和编辑权限，可以查看所有 NetScaler 控制台内容，并且可以执行所有编辑操作。也就是说，用户可以对资源进行添加、修改和删除操作。
- **adminExceptSystem_Pol** 授予用户访问 NetScaler 控制台 GUI 中所有节点的权限，但对“设置”节点的访问权限除外。
- **readonly_polic**y。授予只读权限。用户可以在 NetScaler 控制台上查看所有内容，但无权执行任何操作。
- **appadmin_polic**y。授予在 NetScaler 控制台中访问应用功能的管理权限。绑定到此政策的用户可以：
  - 添加、修改和删除自定义应用程序
  - 启用或禁用服务、服务组和各种虚拟服务器，例如内容切换和缓存重定向
- **appreadonly_policy**。授予对应用程序功能的只读权限。绑定到此策略的用户可以查看应用程序，但不能执行任何添加、修改或删除、启用或禁用操作。

尽管您无法编辑这些预定义策略，但您可以创建自己的（用户定义的）策略。

以前，当您为角色分配策略并将角色绑定到用户组时，可以在 NetScaler 控制台 GUI 中为节点级别的用户组提供权限。例如，您可能只提供对整个 负载平衡 节点的访问权限。您的用户有权访问负载平衡下的所有实体特定子节点（例如，虚拟服务器、服务等），或者他们无权访问负载平衡下的任何节点。

在 NetScaler 控制台 507.x 版本及更高版本中，访问策略管理已扩展到为子节点提供权限。可以为所有子节点（如虚拟服务器、服务、服务组和服务器）配置访问策略设置。

目前，您只能为负载平衡节点下的子节点以及 **GSLB** 节点下的子节点提供这种精细级别的访问权限。

例如，作为管理员，您可能希望向用户授予访问权限，仅允许其查看虚拟服务器，而不能查看 负载平衡 节点中的后端服务、服务组和应用程序服务器。分配了此类策略的用户只能访问虚拟服务器。

要创建用户定义的访问策略，请执行以下操作：

1. 在 NetScaler 控制台 GUI 中，导航 到 设置 > 用户和角色 > 访问策略。
2. 单击添加。
3. 在“创建访问策略”页上的“策略名称”字段中，输入策略的名称，然后在“策略描述”字段中输入描述。

   权 限 部分列出了所有 NetScaler 控制台功能，以及用于指定只读、启用-禁用或编辑权限的选项。

   a) 单击 (+) 图标将每个功能组扩展为许多功能。

   b) 选中功能名称旁边的权限复选框以向用户授予权限。

      - 查看：此选项允许用户在 NetScaler 控制台中查看该功能。
      - 启用**-**禁用：此选项仅适用于允许在 NetScaler 控制台上启用或禁用操作的 网络功能功能。用户可以启用或禁用该功能。用户还可以执行“立即投票”操作。

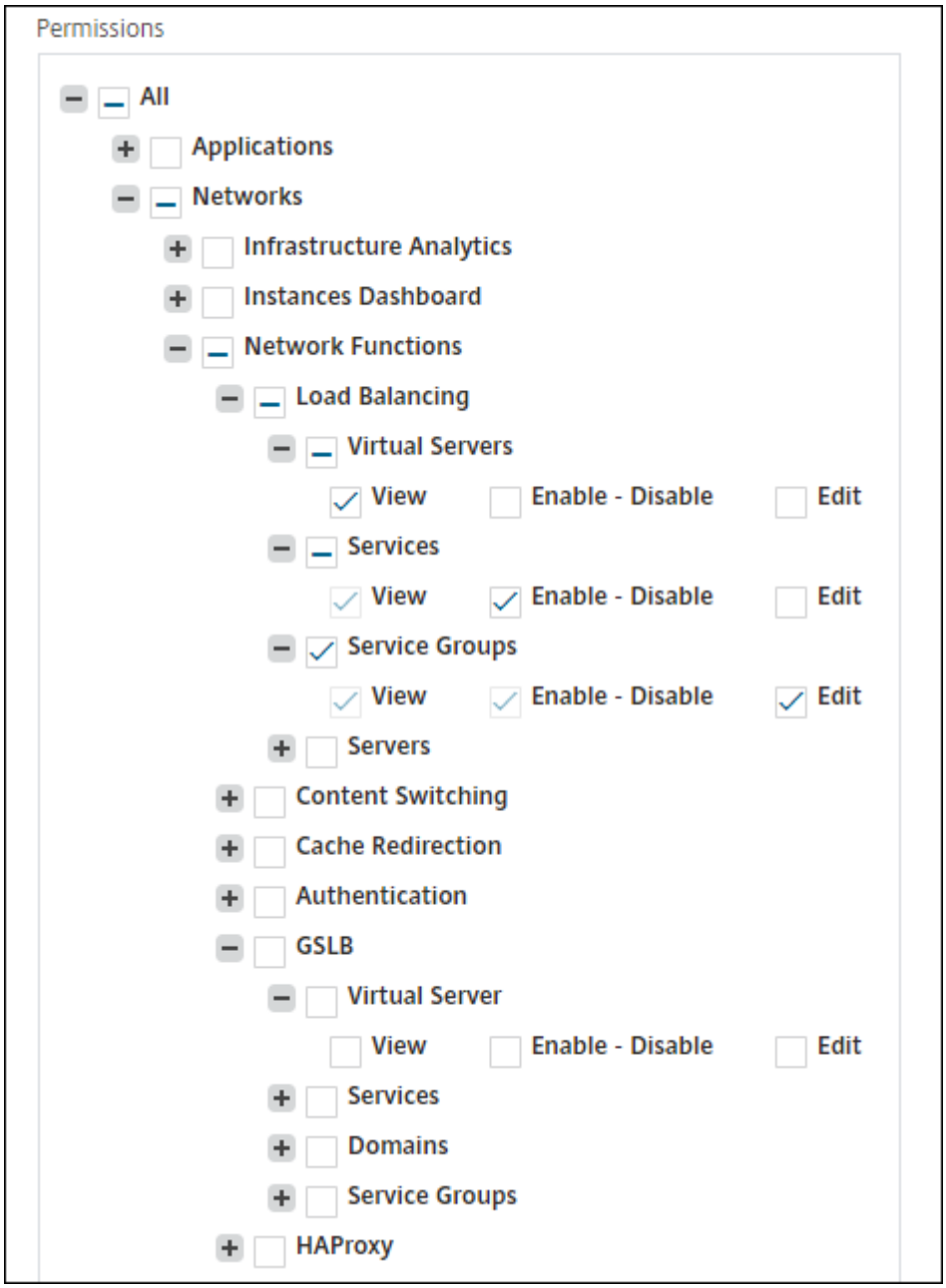
        向用户授予“启用**-**禁用”权限时，也会授予“查看”权限。您不能取消选择此选项。
      - 编辑：此选项向用户授予完全访问权限。用户可以修改该功能及其功能。

        如果您授予“编辑”权限，则会同时授予“查看”和“启用**-**禁用”权限。您不能取消选择自动选择的选项。

如果选中该功能复选框，它将选择该功能的所有权限。

> 注意：
>
> 展开 负载平衡 和 **GSLB** 以查看更多配置选项。

在下图中，负载平衡功能的配置选项具有不同的权限：



“查 看”权限授予用户使用 虚拟服务器 功能。用户可以在 NetScaler 控制台中查看负载平衡虚拟服务器。要查看虚拟服务器，请导航到 基础结构 **>** 网络功能 **>** 负载平衡，然后选择 虚拟服务器 选项卡。

向用户授予 服务 功能的 启用**-**禁 用权限。此权限还授予“查 看”权限。用户可以启用或禁用绑定到负载平衡虚拟

服务器的服务。此外，用户可以对服务执行 立即轮询 操作。要启用或禁用服务，请导航到 基础结构 **>** 网络功能 **>** 负载平衡，然后选择 服务 选项卡。

> 注意：
>
> 如果用户具有“启用-禁用”权限，则在以下页面中限制对服务的启用或禁用操作：
>
> a) 导航到 基础结构 **>** 网络功能。
>
> b) 选择一个虚拟服务器，然后单击 配置。
>
> c) 选择负 载平衡虚拟服务器服务绑定 页面。
> 如果您选择“启 用”或“禁用”，则此页面会显示一条错误消息。

“编辑”权限被授予用户使用“服务组”功能。此权限授予完全访问权限，授予了“查看”和“启用-禁用”权限。用户可以修改绑定到负载平衡虚拟服务器的服务组。要编辑服务组，请导航到 基础结构 **>** 网络功能 **>** 负载平衡，然后选择 服务组 选项卡。

4. 单击创建。

> 注意：
>
> 选择“编辑”可能会在内部分配相关权限，这些权限在“权限”部分中未显示为启用。例如，当您启用故障管理的编辑权限时，NetScaler 控制台会在内部提供配置邮件配置文件或创建 SMTP 服务器设置的权限，以便用户可以将报告作为邮件发送。

向用户授予样书权限

您可以创建访问策略来授予样书权限，例如导入、删除、下载等。

> 注意：
>
> 当您授予其他样书权限时，“查看”权限会自动启用。

在 **NetScaler** 控制台上配置角色

在 NetScaler 控制台中，每个角色都绑定到一个或多个访问策略。您可以在策略与角色之间定义一对一、一对多和多对多关系。您可以将一个角色绑定到多个策略，也可以将多个角色绑定到一个策略。

例如，一个角色可能绑定到两个策略，其中一个策略定义对一个功能的访问权限，另一个策略定义对另一个功能的访问权限。一种策略可能授予在 NetScaler 控制台中添加 NetScaler 实例的权限，另一种策略可能授予创建和部署样书以及配置 NetScaler 实例的权限。

当多个策略为单个要素定义编辑和只读权限时，编辑权限优先于只读权限。

NetScaler 控制台提供五种预定义角色：

- **admin_role**。可以访问所有 NetScaler 控制台功能。（此角色绑定到 `adminpolicy`。）

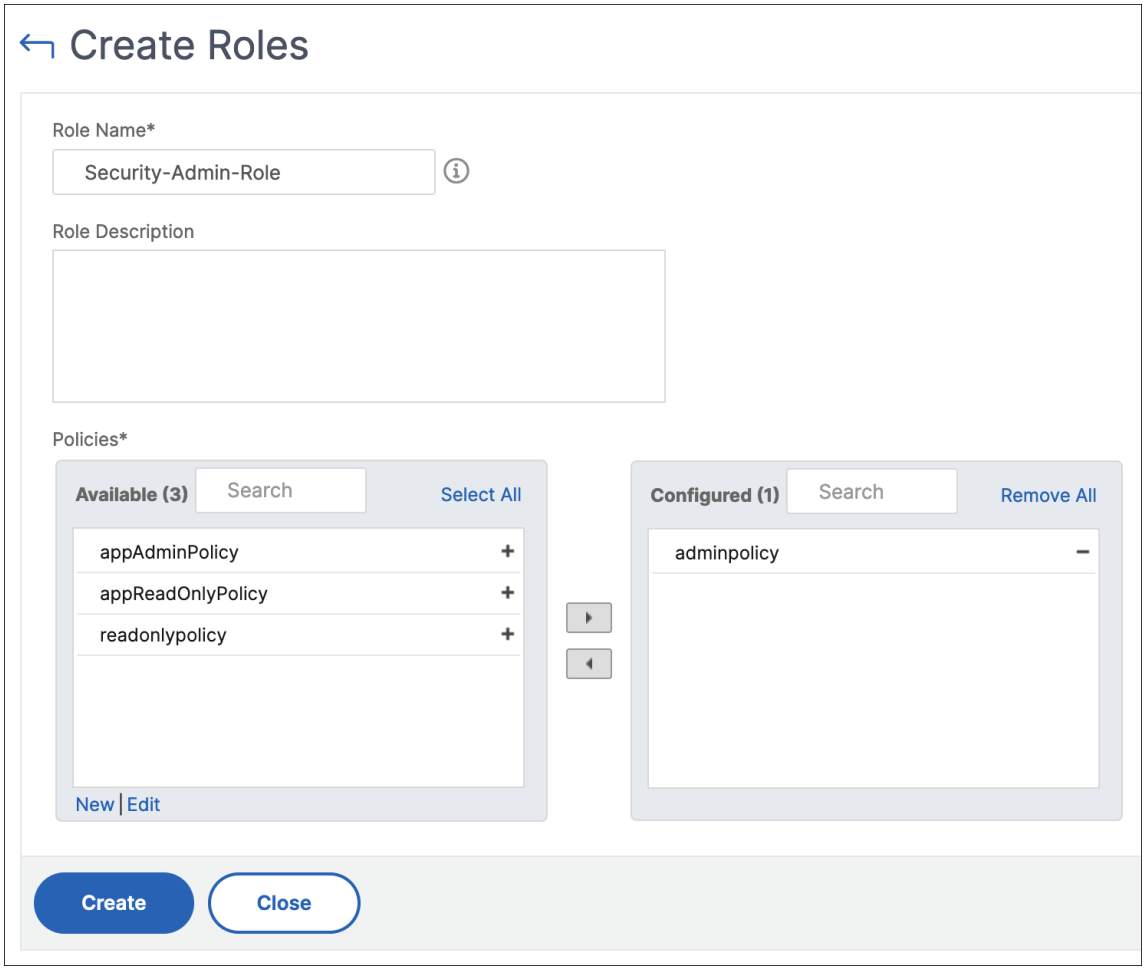
- **adminExceptSystem_rol**e 除设置权限外，有权访问 NetScaler 控制台 GUI。（此角色绑定到 adminExceptSystem_Policy）
- **readonly_role**。拥有只读访问权限。（此角色绑定到 `readonlypolicy`。）
- **appAdmin_role**。只能对 NetScaler 控制台中的应用功能具有管理权限。（此角色绑定到 appAdminPolicy。）
- **appReadonly_role**。对应用程序功能具有只读访问权限。（此角色绑定到 appReadOnlyPolicy。）

尽管您无法编辑预定义角色，但可以创建自己的（用户定义的）角色。

要创建角色并为其分配策略，请执行以下操作：

1. 在 NetScaler 控制台 GUI 中，导航 到 设置 > 用户和角色 > 角色。
2. 单击添加。
3. 在 创建角色 页面的 角色名称 字段中，输入角色的名称，并在角色描述字段中提供 描述（可选）。
4. 在 策略 部分中，将一个或多个策略添加到 已配置 列表中。

   > 注意：
   >
   > 这些策略以所有租户唯一的租户 ID（例如 `maasdocfour`）为前缀。



> 注意：
>
> 您可以通过单击“新建”来创建访问策略，也可以导航到“**** 设置” > “用户和角色” > “访问策略”，**** 然后创建策略。

5. 单击创建。

在 **NetScaler** 控制台上配置组

在 NetScaler 控制台中，组可以同时具有功能级别和资源级访问权限。例如，一组用户可能只能访问选定的 NetScaler 实例；另一组用户只能访问选定的几个应用程序，依此类推。

创建组时，您可以为组分配角色、提供对组的应用程序级别访问权限以及将用户分配给组。在 NetScaler 控制台中，该组中的所有用户都被分配了相同的访问权限。

您可以在 NetScaler 控制台中管理各个网络功能实体级别的用户访问权限。您可以在实体级别为用户或组动态分配特定权限。

NetScaler 控制台将虚拟服务器、服务、服务组和服务器视为网络功能实体。

- 虚拟服务器（应用程序） -负载平衡 (`lb`)、GSLB、上下文切换 (`CS`)、缓存重定向 (`CR`)、身份验证 (`Auth`) 和 NetScaler Gateway (`vpn`)
- 服务 -负载平衡和 GSLB 服务
- 服务组 -负载平衡和 GSLB 服务组
- 服务器 -负载平衡服务器

要创建组，请执行以下操作：

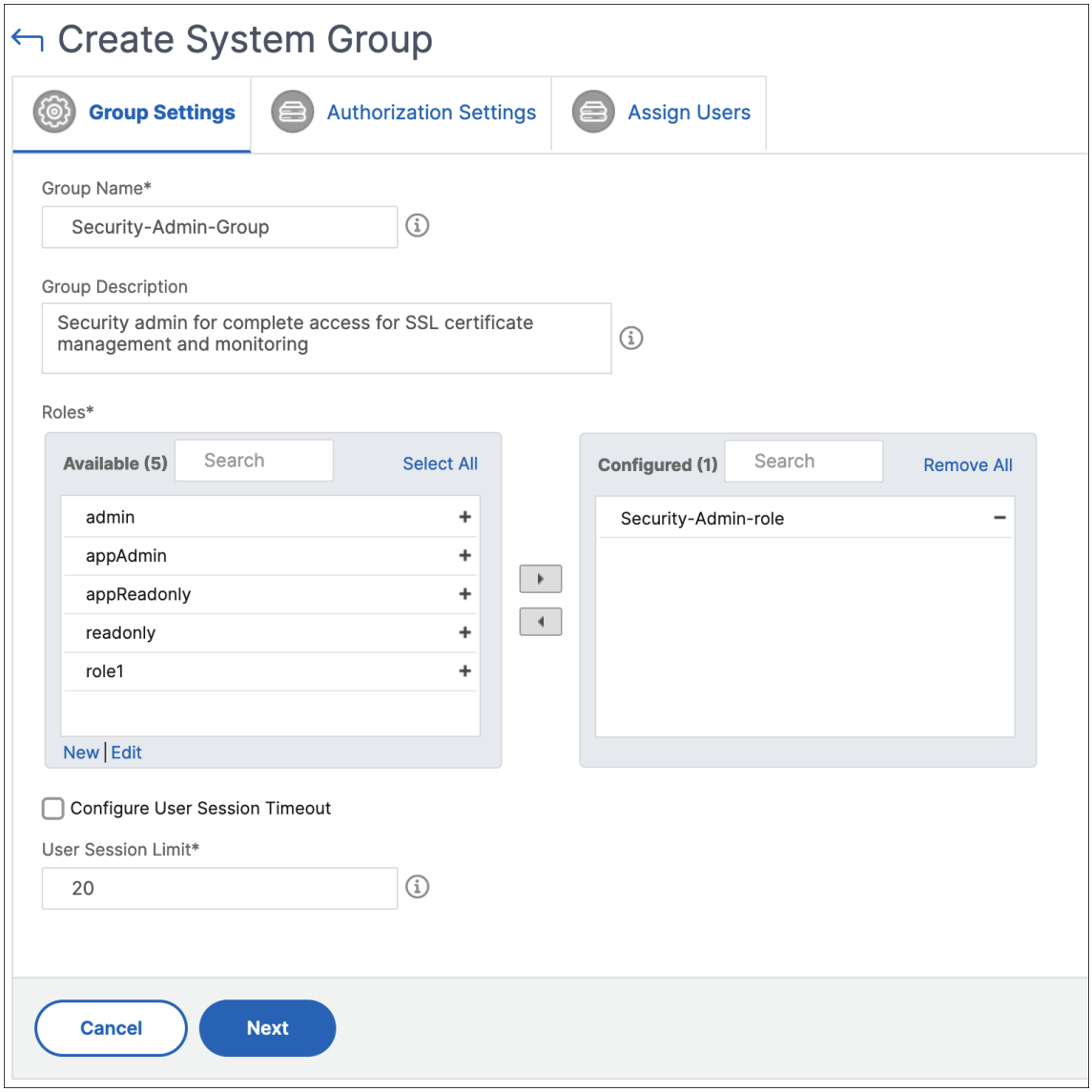
1. 在 NetScaler 控制台中，导航到设置 > 用户和角色 > 组。
2. 单击添加。

   屏幕上将显示“创建系统组”页面。
3. 在 组名称 字段中，输入组的名称。
4. 在“组描述”字段中，键入组的描述。提供良好的描述可以帮助您了解组的角色和职能。
5. 在“角色”部分中，将一个或多个角色移至“已配置”列表。

   > 注意：
   >
   > 角色以所有租户唯一的租户 ID（例如 `maasdocfour`）为前缀。

6. 在“可用”列表中，您可以单击“新 建”或“编辑”，然后创建或修改角色。

   或者，您可以导航到“设置” > “用户和角色” > “用户”，然后创建或修改用户。



7. 单击下一步。
8. 在 授权设置 选项卡中，您可以从以下类别中选择资源：

   - **AutoScale** 组
   - 实例
   - 应用程序
   - 配置模板
   - **IPAM** 提供商和网络
   - 样书
   - 配置包
   - 域名

   从用户可以访问的类别中选择特定资源。

AutoScale 组：

要选择用户可以查看或管理的特定 AutoScale 组，请执行以下操作：

a) 清除“所有 **AutoScale** 组”复选框，然后单击“添加 **AutoScale** 组”。

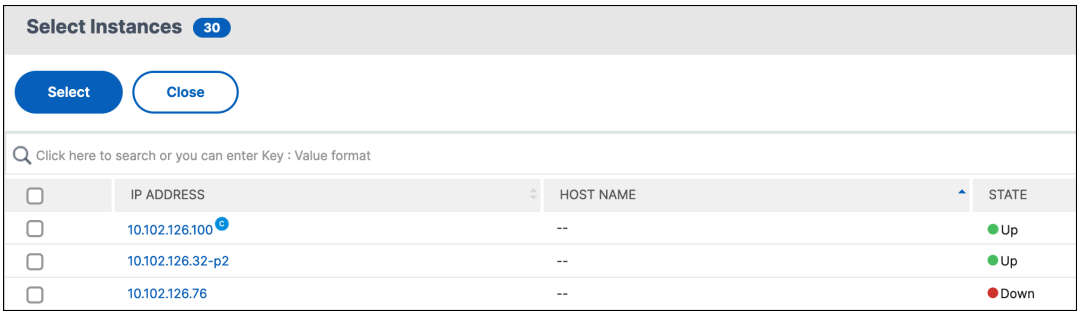
b) 从列表中选择所需的 AutoScale 组，然后单击“确定”。

实例：

要选择用户可以查看或管理的特定实例，请执行以下操作：

a) 清除“所有实例”复选框，然后单击“选择实例”。

b) 从列表中选择所需的实例，然后单击“确定”。

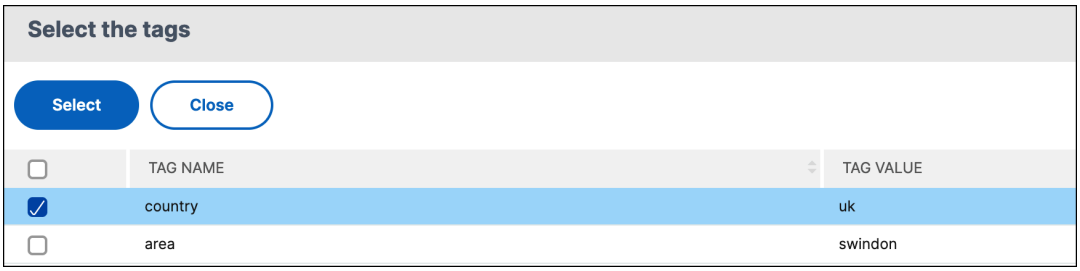


标记**:**

要授权用户根据关联标签查看或管理特定实例，请执行以下操作：

a) 清除“所有实例”复选框，然后单击“选择标签”。

b) 从列表中选择所需的标签，然后单击“确定”。



之后，当您将更多实例与所选标签关联时，授权用户会自动获得对新实例的访问权限。

有关标签以及将标签与实例关联的更多信息，请参阅 如何创建标签和分配给实例。

应用程序：

“选择应用程序”列表允许您向用户授予所需应用程序的访问权限。

您可以向应用程序授予访问权限，而无需选择其实例。因为应用程序独立于其实例来授予用户访问权限。

当您向用户授予应用程序访问权限时，无论选择何种实例，该用户都有权仅访问该应用程序。

此列表为您提供了以下选项：

- 所有应用程序：默认情况下，此选项处于选中状态。它添加了 NetScaler 控制台中存在的所有应用程序。
- 选定实例的所有应用程序：仅当您从“所有 实例”类别中选择实例时，此选项才会出现。它添加了选定实例上存在的所有应用程序。
- 特定应用程序：此选项允许您添加希望用户访问的所需应用程序。单击 添加应用程序”，然后从列表中选择所需的应用程序。
- 选择单个实体类型：此选项允许您选择特定类型的网络函数实体和相应实体。

  您可以添加单个实体，也可以选择所需实体类型下的所有实体，以向用户授予访问权限。

  同时应用于绑定实体 选项对绑定到选定实体类型的实体进行授权。例如，如果您选择一个应用程序并选择“同时应用于绑定实体”，则 NetScaler 控制台会对绑定到所选应用程序的所有实体进行授权。

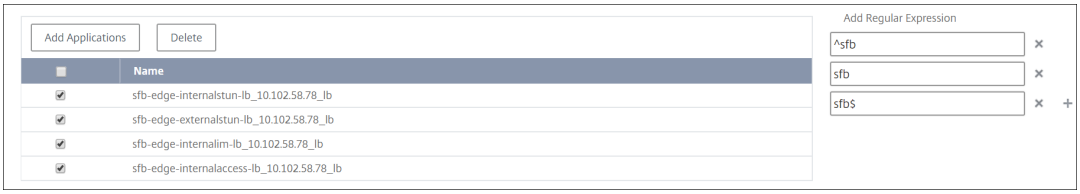
  > 注意：
  >
  > 如果要授权绑定实体，请确保只选择了一种实体类型。

您可以使用正则表达式搜索和添加符合组正则表达式条件的网络函数实体。指定的正则表达式保留在 NetScaler 控制台中。要添加正则表达式，请执行以下步骤：

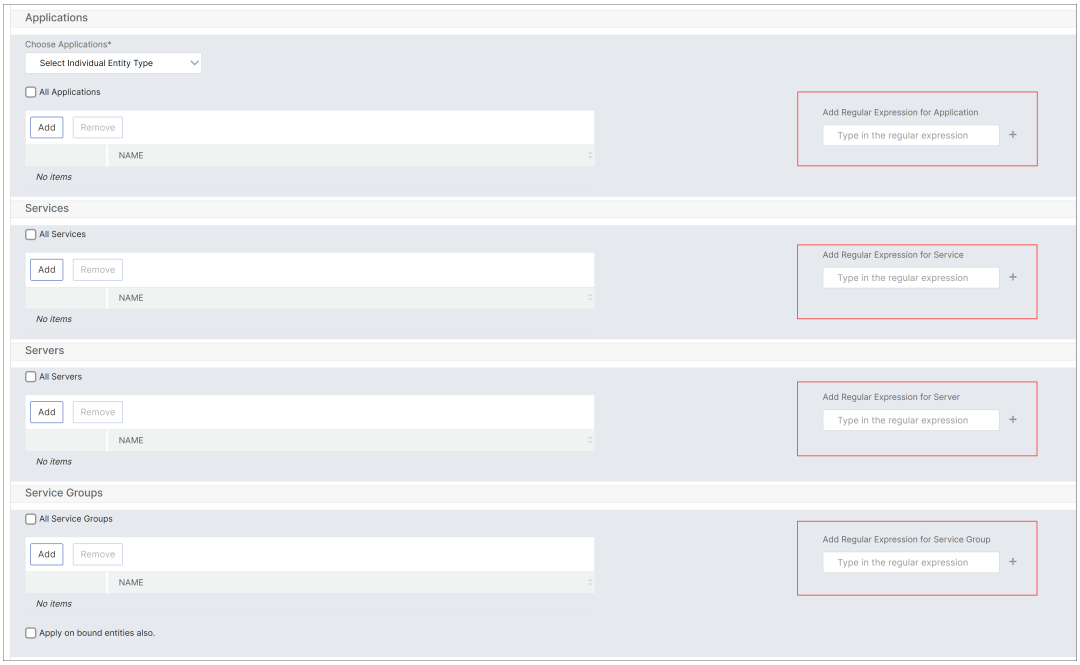
a) 单击“添加正则表达式”。

b) 在文本框中指定正则表达式。

下图说明了在选择“特定应用程序”选项时如何使用正则表达式添加应用程序：



下图说明了在选择“选择单个实体类型”选项时如何使用正则表达式添加网络功能实体：



如果要添加更多正则表达式，请单击 **+** 图标。

> 注意：
>
> 正则表达式仅匹配服务器实体类型的服务器名称，而不匹配服务器 IP 地址。

如果您为已发现的 实体选择“同时应用于绑定 实体”选项，则用户可以自动访问绑定到已发现实体的实体。

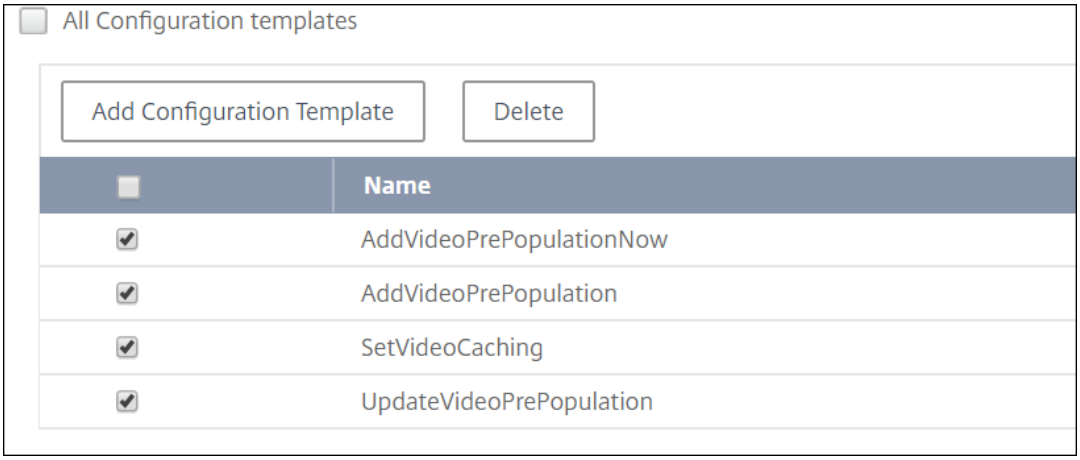
正则表达式存储在系统中以更新授权范围。当新实体与其实体类型的正则表达式匹配时，NetScaler 控制台会将授权范围更新为新实体。

配置模板：

如果要选择用户可以查看或管理的特定配置模板，请执行以下步骤：

a) 清除“所有配置模板”，然后单击“添加配置模板”。

b) 从列表中选择所需的模板，然后单击“确定”。



IPAM 提供商和网络：

如果要添加用户可以查看或管理的特定 IPAM 提供程序和网络，请执行以下操作：

- 添加提供商 -清除 所有提供商，然后单击“添加提供商”。您可以选择所需的提供商，然后单击确定。
- 添加网络 -清除 所有网络，然后单击“添加网络”。您可以选择所需的网络，然后单击确定。

样书：

如果要选择用户可以查看或管理的特定样书，请执行以下步骤：

a) 清除“所有样书”复选框，然后单击“将样式手册添加到组”。您可以选择单个样书，也可以指定筛选器查询来授权样书。

如果要选择单个样书，请从“单个样书”窗格中选择样书，然后单击保存所选内容。

如果要使用查询来搜索样书，请选择自定义过滤器窗格。查询是键值对的字符串，其中键是 `name`、`namespace` 和 `version`。

您也可以使用正则表达式作为值来搜索和添加符合组正则表达式条件的样书。用于搜索样书的自定义筛选器查询同时支持 `And` 和 `Or` 操作。

示例：

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
     version=1.0
```

此查询列出了满足以下条件的样书：

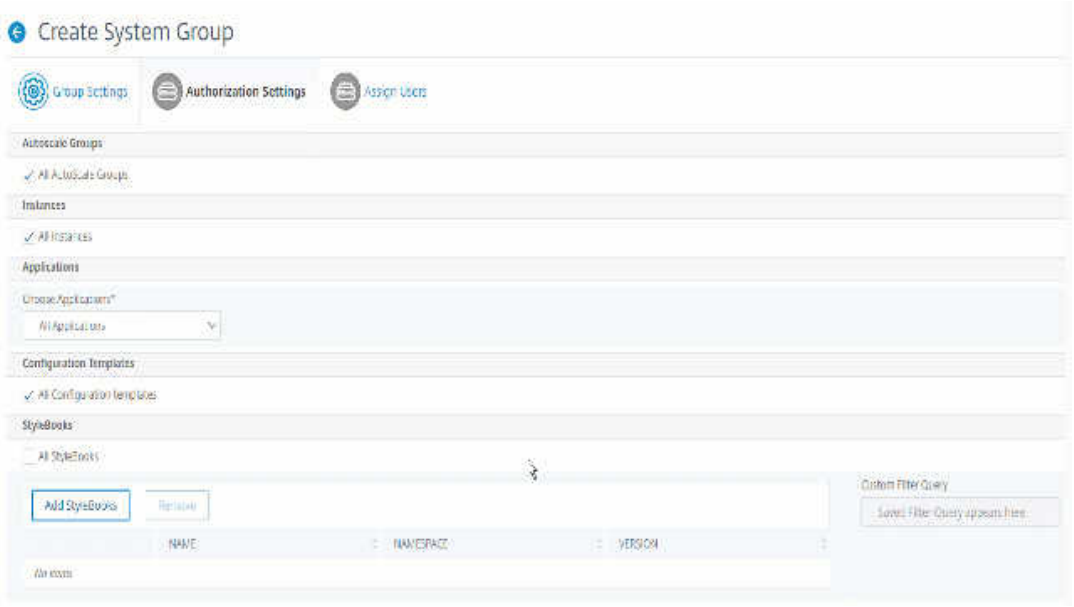
- 样书名称是 `lb-mon` 或 `lb`。
- 样书名称空间是 `com.citrix.adc.stylebooks`。
- 样书版本是 `1.0`。

在为键表达式定义的值表达式之间使用 `Or` 操作。

示例：

- `name=lb-mon|lb` 查询是有效的。它返回名称为 `lb-mon` 或 `lb` 的样书。
- `name=lb-mon | version=1.0` 查询无效。

按 `Enter` 以查看搜索结果，然后单击 保存查询。



保存的查询将显示在 自定义筛选器查询中。根据保存的查询，NetScaler 控制台允许用户访问这些样书。

b) 从列表中选择所需的样书，然后单击“确定”。

您可以在创建组并将用户添加到该组时选择所需的样书。当用户选择允许的样书时，也会选择所有相关样书。

配置包：

在配置包中，选择以下选项之一：

- 所有配置：默认情况下，此选项处于选中状态。它允许用户管理 ADM 中的所有配置。
- 所选样书的所有配置：此选项添加所选样书的所有配置包。
- 特定配置：此选项允许您添加任何样书的特定配置。
- 用户组创建的所有配置：此选项仅允许用户访问由同一组的用户创建的配置。

在创建组并将用户分配到该组时，您可以选择适用的配置包。

域名：

如果要选择用户可以查看或管理的特定域名，请执行以下步骤：

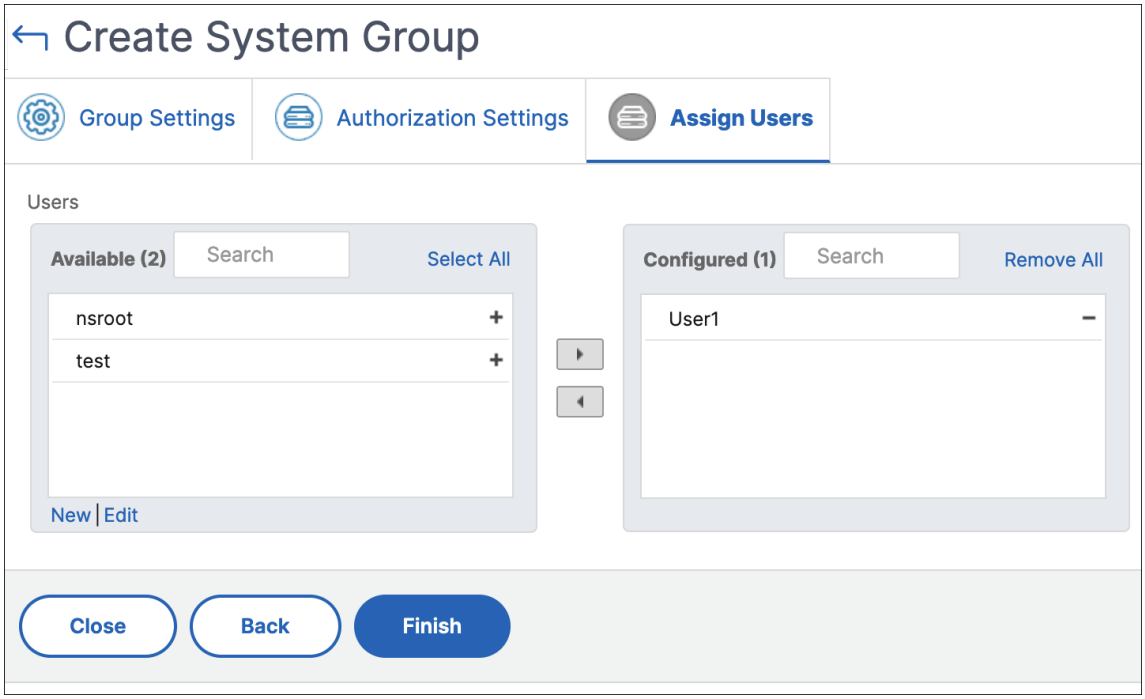
a) 清除“所有域名”复选框，然后单击“添加域名”。

b) 从列表中选择所需的域名，然后单击“确定”。

c) 单击创建组。

d) 在“分配用户”部分，在“可用”列表中选择用户，然后将该用户添加到“已配置”列表中。

> 注意：
>
> 您也可以通过单击“新建”来添加 新用户。



a) 单击完成。

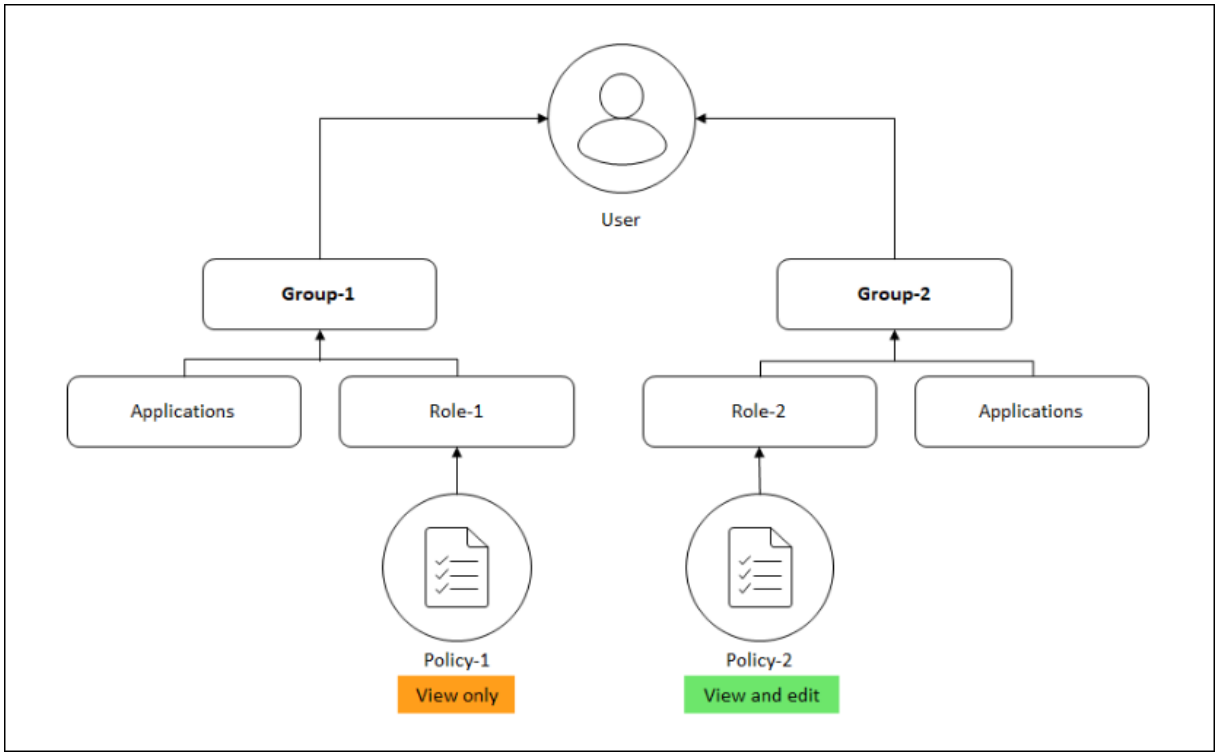
用户访问权限如何根据授权范围进行更改

当管理员将用户添加到具有不同访问策略设置的组时，该用户将被映射到多个授权作用域和访问策略。

在这种情况下，NetScaler 控制台根据特定的授权范围向用户授予对应用程序的访问权限。

考虑分配给具有两个策略策略 1 和策略 2 的组的用户。

- 策略 **1** —仅查看应用程序的权限。
- **Policy-2** -查看和编辑应用程序的权限。



用户可以查看 Policy-1 中指定的应用程序。此外，此用户还可以查看和编辑策略 2 中指定的应用程序。对组 1 应用程序的编辑访问受到限制，因为它不在组 1 授权范围内。

限制

以下 NetScaler 控制台功能不完全支持 RBAC：

- 分析 - 分析模块不完全支持 RBAC。RBAC 支持仅限于实例级别，不适用于 Gateway Insight、HDX Insight 和 Security Insight 分析模块中的应用程序级别。
  - 示例 1：基于实例的 RBAC（支持）。分配了几个实例的管理员只能在 **HDX Insight** > 设备下看到这些实例，在 **HDX Insight** > 应用程序下只能看到相应的虚拟服务器，因为实例级别支持 RBAC。
  - 示例 2：基于应用程序的 RBAC（不支持）。分配了几个应用程序的管理员可以在 **HDX Insight** > 应用程序 下查看所有虚拟服务器，但无法访问它们，因为应用程序级别不支持 RBAC。
- 样书—样书不完全支持 RBAC。
  - 考虑这样一种情况：许多用户可以访问单个样书，但对不同的 NetScaler 实例具有访问权限。用户可以在自己的实例上创建和更新配置包，因为除了自己的实例外，他们无权访问其他实例。但是，他们仍然可以查看在 NetScaler 实例上创建的配置包和对象，而不是自己的配置包和对象。

为托管 **NetScaler** 实例分配网络配置文件

July 17, 2024

当您在 NetScaler 控制台中为虚拟服务器启用分析或指标收集器时，来自 NetScaler 的 AppFlow 或指标数据将通过 NetScaler 子网 IP 地址 (SNIP) 导出到 NetScaler 控制台。在某些情况下，SNIP 可能会因为网络中的防火墙而被阻止。在这种情况下，您可能必须使用不同的 IP 地址。有关网络配置文件的更多信息，请参阅使用指定的源 IP 进行后端通信。

您可以通过 NetScaler 控制台向 NetScaler 实例分配网络配置文件，以将 AppFlow 数据从 NetScaler 导出到 NetScaler 控制台。

必备条件

请确保：

- NetScaler 实例版本为 **13.0-**48.4 或更高版本。
- 网络配置文件是在 NetScaler 实例中配置的。

要在 NetScaler 控制台中分配网络配置文件，请执行以下操作：

1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 选择实例，然后从“选择操作”列表中：
    - 单击“配置网络配置文件”为 AppFlow 分配网络配置文件。
    - 单击“为指标收集器配置网络配置文件”为指标收集器分配网络配置文件。
3. 从列表中选择一个网络配置文件，然后单击“应用”。

> 注意：
>
> - 对于 AppFlow，请确保在为实例分配网络配置文件之前禁用所有虚拟服务器的分析。
> - 对于指标收集器，请确保在为实例分配网络配置文件之前禁用所有虚拟服务器的指标。

数据存储管理

January 29, 2024

了解在 NetScaler 控制台中使用了哪些功能以及每种功能的数据使用情况非常重要。数据存储管理 控制面板可实现此目的，可用作您的可视化工具，使您能够了解存储在 NetScaler 控制台数据库中的各种功能总数据。控制板还会显示消耗的存储空间是否在指定的限制范围内，或者是否超过了授权的存储空间。

作为管理员，您可以在“数据存储管理”控制面板中执行以下任务：

- 查看过去 30 天的数据存储消耗-过去 30 天的数据存储趋势存储在 NetScaler 控制台数据库中。这些趋势以图形或表格形式提供。这些趋势显示了在 NetScaler 控制台中计划的修剪周期结束后，流入了多少数据以及存储了多少数据。
- 查看数据摄取状态-只要消耗的存储空间在授权存储空间的限制范围内，就会发生数据摄取活动。当消耗的存储空间超过授权的存储空间时，数据活动将暂停。
- 发送通知-您可以将通知设置为在已消耗的存储空间达到授权存储空间的 75% 或 100% 时发送，从而允许用户管理其存储空间。
- 灵活管理数据存储空间-您可以通过修剪您认为适合删除或减少的数据，在存储的数据中创建更多空间。

导航到“设置”**>**“数据存储管理”以查看您的数据存储控制面板。

以下各节概述了如何使用数据存储管理控制板进行有效的数据存储管理：

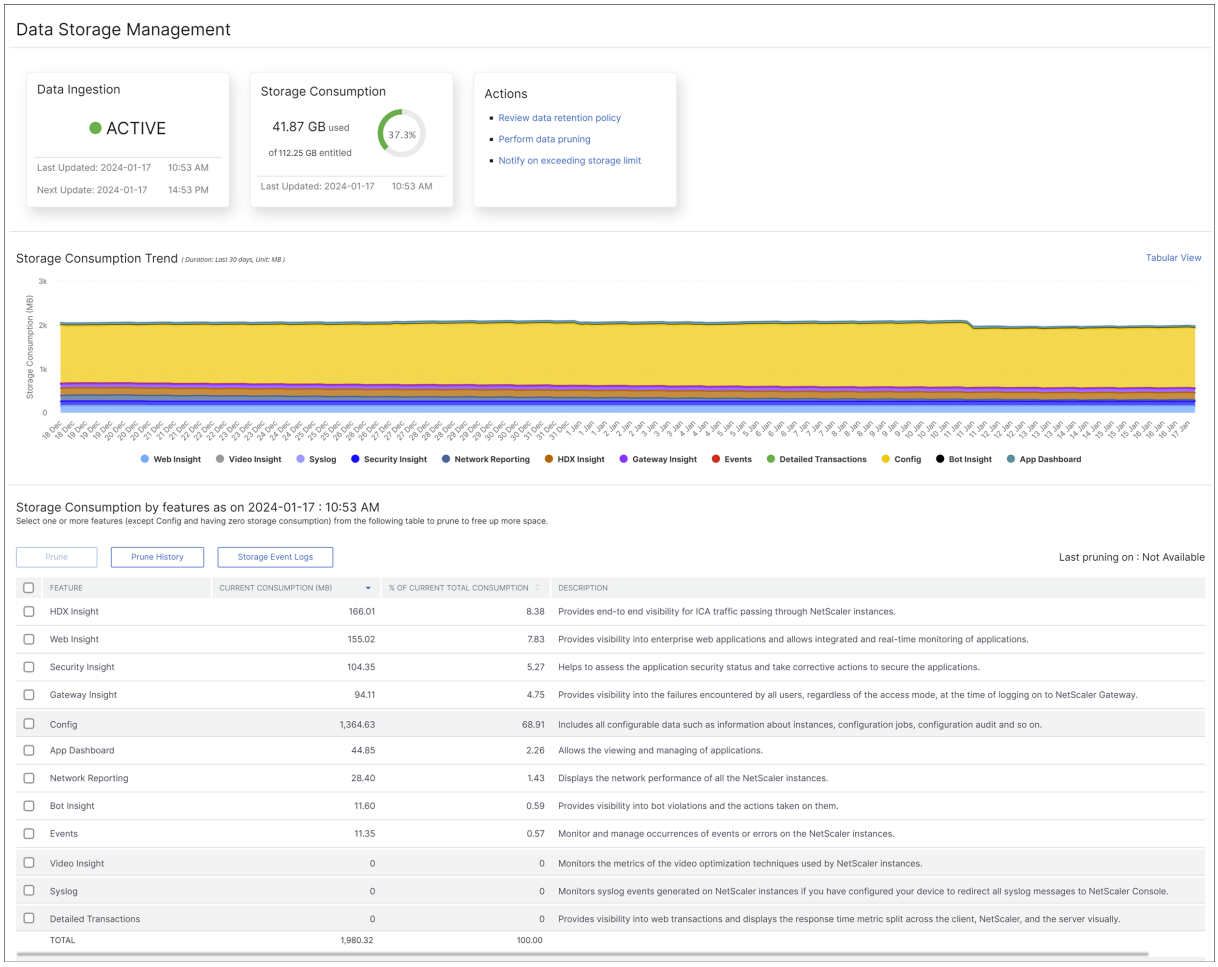
- 了解您的数据存储 - 本部分可帮助您了解如何使用控制板查看有关数据存储的信息。
- 管理您的数据存储 - 本部分提供有关您可以在控制面板中采取哪些操作来管理数据存储的信息。

了解您的数据存储

May 9, 2024

您可以使用 NetScaler 控制台中的“数据存储管理”控制面板来查看数据和图表，以帮助您跟踪数据存储使用情况。

要监视您的数据存储消耗，请导航至“设置”**>**“数据存储管理”。



“数据存储管理”控制板显示以下信息：

- 您的数据摄取活动状态
- 总存储消耗
- 数据修剪状态
- 存储消耗趋势
- 按功能划分的存储消耗

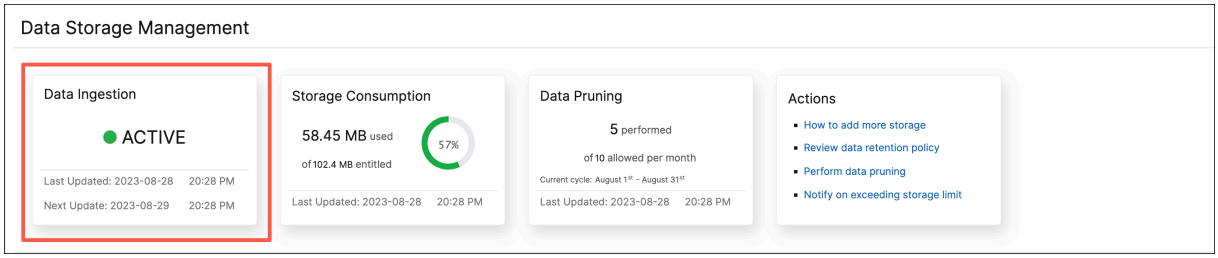
您的数据摄取活动状态

数据摄取是指将各种功能（如事件、系统日志、网络报告等）的所有托管 NetScaler 实例中的大型和各种数据导入 NetScaler 控制台存储的过程。

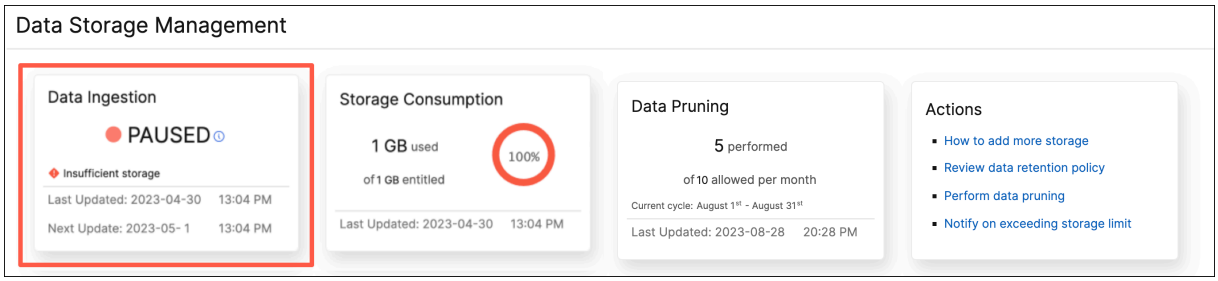
数据摄取状态指示 NetScaler 控制台是否正在从 NetScaler 实例收集统计信息。只要消耗的存储空间位于授权的存储空间内，数据摄取活动就会继续。当消耗量超过授权存储空间时，数据提取将暂停。

查看“数据摄取”图块以了解数据摄取的当前状态。此图块显示以下两种状态之一：

- 活动 -数据摄取活动正在进行中。



- 已暂停 -由于消耗的存储空间超过了授权的存储空间，因此数据摄取活动已暂停。



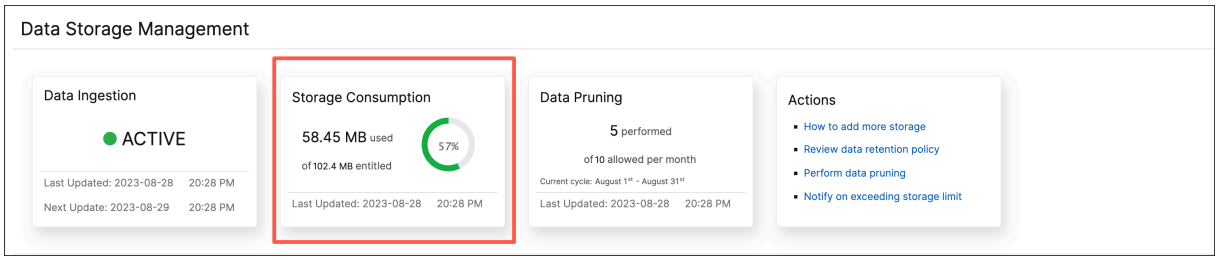
如何恢复暂停的数据摄取

要恢复数据摄取活动，您可以执行以下任一操作：

- 添加更多数据存储空间。
- 执行数据修剪。

总存储消耗

要快速了解您的数据存储，请查看“存储消耗”图块。



“存储消耗”图块显示部署中所有功能使用的总存储空间。

将鼠标悬停在甜甜圈图上方可查看以下内容：

授权存储

授权的存储空间是指根据您的许可证可供您使用的总存储空间。如果您拥有 Express 许可证，则可获得 500 MB 的授权存储空间。如果您拥有高级许可证，则每购买一个 VIP 将获得 500 MB 的存储空间总和，以及无需购买 VIP 即可直接购买的任何额外存储空间。

考虑以下场景：

- 您买了 20 个 VIP。每个 VIP 将获得 500 MB 的免费存储空间。您授权的存储空间为 20*500 = 10 GB。
- 您购买了 20 个 VIP 和 5 GB 的附加存储空间。每个 VIP 将获得 500 MB 的免费存储空间。您授权的存储空间为 20*500 + 5 = 15 GB。

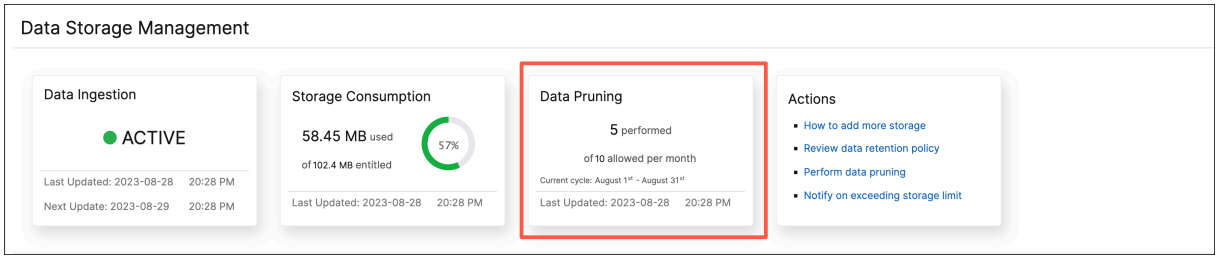
消耗的存储空间

消耗的存储空间是部署中所有功能使用的总存储空间。以下颜色编码标准指定了功能使用的存储量：

- 绿色 -消耗的存储空间少于授权存储空间的 75%。
- 琥珀色 -消耗的存储空间占授权存储空间的 75% 到 99% 之间。
- 红色 -已消耗的存储空间限制已达到或高于当前授权的存储空间。

数据修剪状态

修剪是手动删除数据并释放存储空间的过程。每个日历月允许您修剪 10 个数据。例如，从 7 月 1 日到 7 月 31 日，您可以删除数据 10 次。



要了解您已经用完了多少数据修剪以及还剩多少数据修剪，请查看“数据修剪”图块。

> 注意：
>
> 无论选择了多少要素，每个修剪活动都算作一次数据修剪。

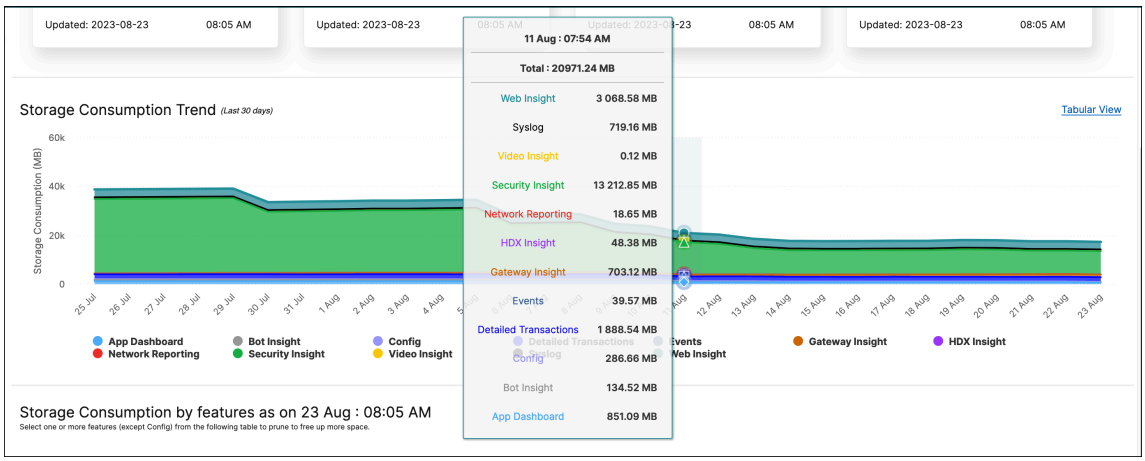
存储消耗趋势

要了解过去 30 天内的数据使用情况，请查看“存储消耗趋势”部分。

存储消耗趋势可让您深入了解在一段时间内哪些功能使用最多或最少的存储空间，并帮助您有效地管理数据存储消耗。

您可以通过以下任一形式查看存储数据趋势：

- 图形视图—显示数据存储在不同的 NetScaler 控制台功能中的分布情况。将鼠标悬停在时间轴上可查看当月任何一天的数据存储信息。



> 注意：
>
> 图 形视图 是默认视图。

- 表格视图 -单击“表格视图”以表格形式显示数据存储信息。

> 注意：
>
> 表格视图允许您使用搜索字段筛选数据。

下表介绍了“存储消耗趋势”部分中显示的字段：

功能	说明
配置	包括所有可配置数据，例如有关实例、配置作业、配置审核等的信息。

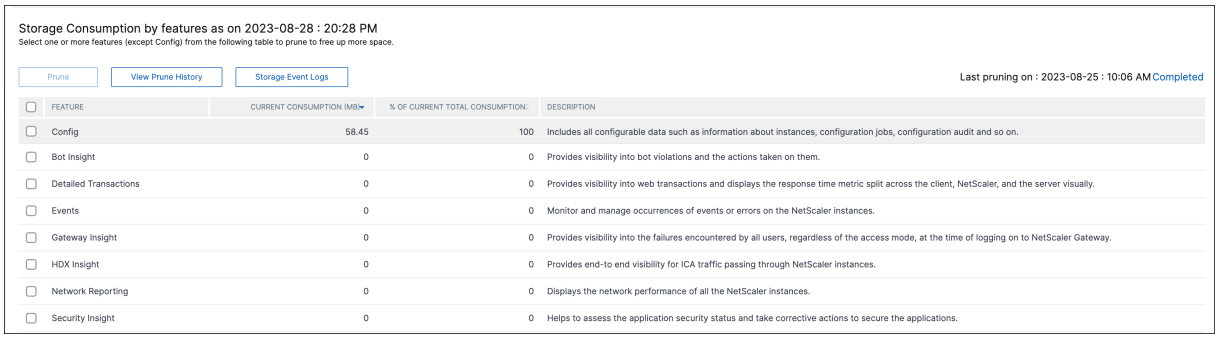
功能	说明
HDX Insight	为通过 NetScaler 的 ICA 流量提供端到端可见性。
网络报告	显示所有 NetScaler 实例的网络性能。
Web Insight	提供企业 Web 应用程序的可见性，并允许对应用程序进行集成、实时监视。
Security Insight	帮助评估应用程序安全状态并采取纠正措施来保护应用程序。
Gateway Insight	提供所有用户在登录 NetScaler Gateway 时遇到的故障的可见性，无论其访问模式如何。
事件	监视和管理 NetScaler 实例上发生的事件或错误。
应用程序控制板	允许查看和管理应用程序。
机器人洞察	提供对机器人违规行为以及对其采取的操作的可见性。
Syslog	如果您已将设备配置为将所有系统日志消息重定向到 NetScaler 控制台，则监视在 NetScaler 实例上生成的系统日志事件。
Video Insight	监视 NetScaler 实例使用的视频优化技术的指标。
详细事务	提供对 Web 事务的可见性，直观地显示客户端、NetScaler 和服务器的响应时间指标。

按功能划分的存储消耗

要详细了解数据存储在不同功能之间的分布情况，请查看 *dd mmm** 部分中的按功能划分的 ** 存储消耗量。

dd mmm 中按功能划分的存储消耗量可帮助您理解：

- NetScaler 控制台中所有不同功能使用的存储空间
- 功能在特定日期消耗的空间百分比



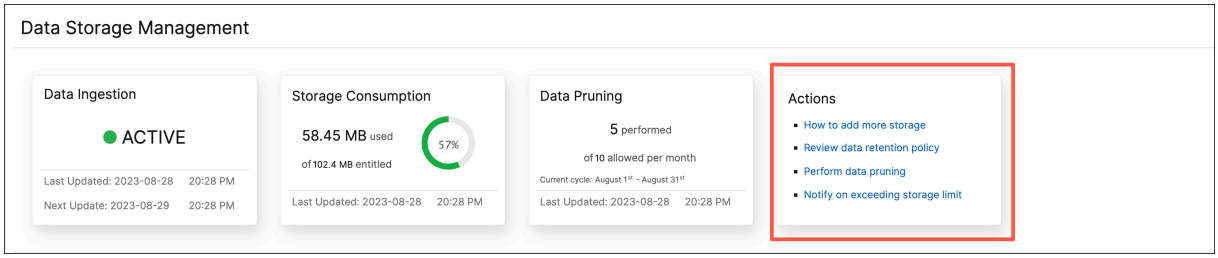
如果要对表格条目进行排序，则对表的标题进行排序。NetScaler 控制台根据所选列中的数据按字母数字顺序对表格进行从上到下排序。要按相反顺序对表格进行排序，请再次单击列标题。

有关修剪数据、修剪历史记录和存储事件日志的信息，请参阅 管理您的数据存储。

管理您的存储空间

July 17, 2024

您可以使用数据存储管理控制面板来观察您的数据存储使用情况，并在数据存储超过许可限制时采取必要的措施来清理空间或增加存储空间。



“操作”图块显示了您可以采取哪些建议步骤来管理存储容量：

- 查看数据保留政策
- 执行数据修剪
- 超过存储限制时发出通知

当您消耗的存储空间达到许可存储空间的 100% 时，数据摄取活动将暂停，数据将不再存储在 NetScaler 控制台中。

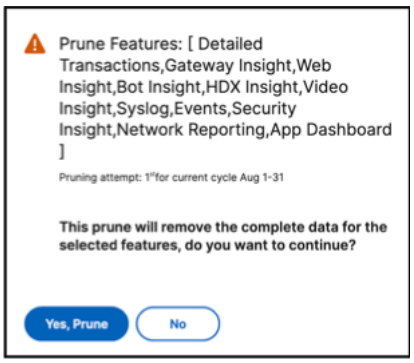
执行数据修剪

修剪数据以优化存储资源并获得更多存储空间。除了腾出空间外，数据修剪还能提高数据质量并缩短处理时间。我们建议您定期查看和清除不必要的数据。此过程可确保谨慎使用您的资源，并且 NetScaler 控制台灵活且响应迅速。

要修剪您的数据，请执行以下操作：

1. 在“数据存储管理”页面中，向下滚动到 ***yyyy-mm-dd*** 按功能划分的存储消耗部分。
2. 选择一个或多个功能，然后单击“修剪”。您无法选择“配置”，因为它包含所有系统配置。

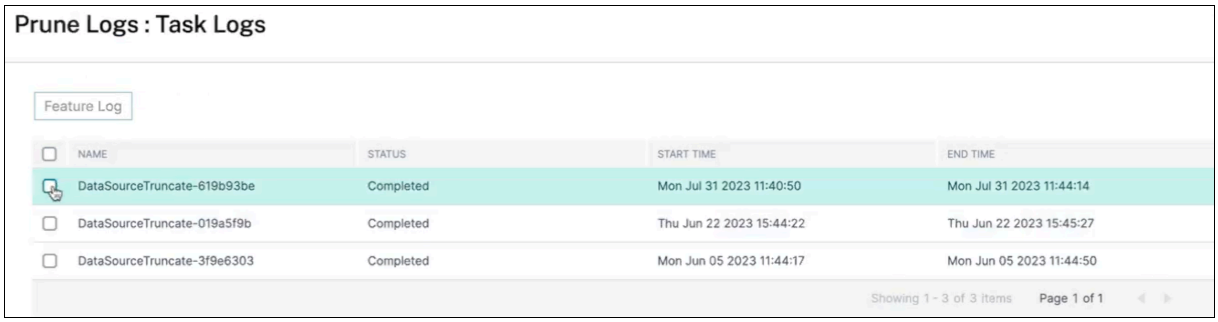
   弹出窗口提示您确认是否要删除所选要素的所有数据。单击“是，修剪”。



> 注意：
>
> 弹出窗口还会显示有关您当前修剪尝试的信息。

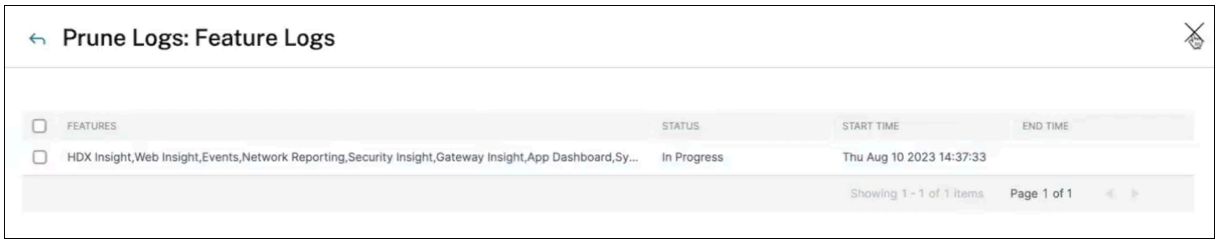
查看修剪历史记录

单击“查看删除历史记录”以获取有关您在 NetScaler 控制台中所做的所有修剪活动的详细信息。



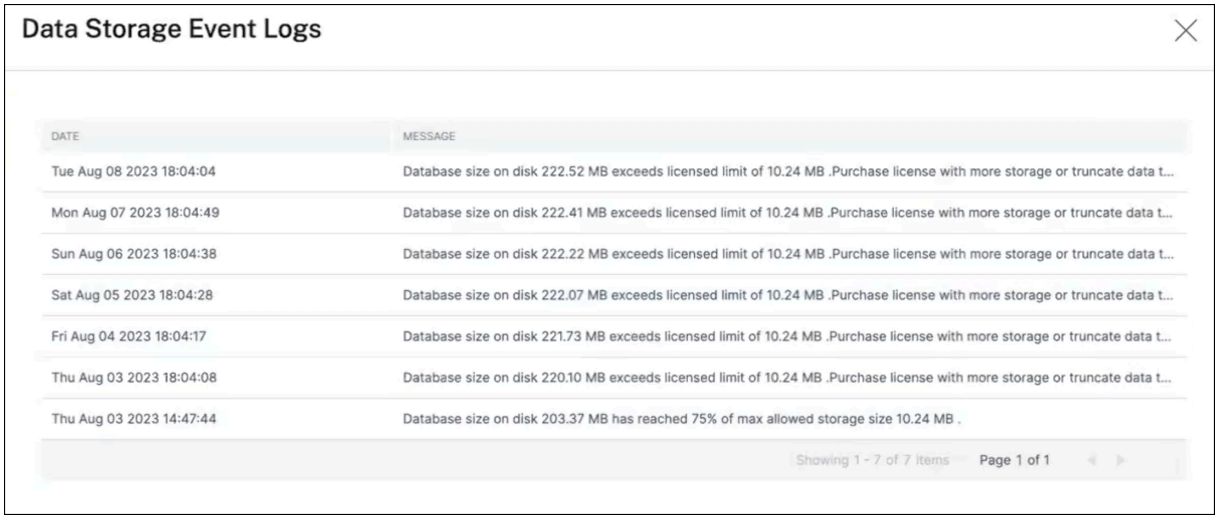
“修剪日志：任务日志”页面显示所有修剪任务的列表，包括其各自的状态、开始时间和结束时间。

要了解每个修剪操作中删除了哪些功能，请选择一项任务并单击“功能日志”。



查看存储事件日志

单击“存储事件日志”，深入了解您的数据超过或达到许可限制的 75% 的所有时间。



查看数据保留政策

数据保留策略是指一组规则和配置，用于确定 NetScaler 控制台在一段时间内如何管理和维护历史数据。此政策概述了数据在自动删除之前要存储多长时间。

如果您想减少所有不同功能使用的存储空间，可以更改数据在 NetScaler 控制台中的保存时间。

使用“数据保留策略”页面编辑以下各项的数据存储设置：

- 事件消息
- 系统日志消息
- 网络报告数据

有关数据存储设置的更多信息，请参阅数据保留政策。

超出存储限制时发出通知

您可以为 NetScaler 控制台设置通知，以便在数据存储容量超过指定限制时向您发送警报。

要查看和配置系统通知，请执行以下操作：

1. 在操作图块中，单击超过存储限制时通知。
2. 在“配置系统通知”页面的“系统事件类别”下，确保选择“**DataStorageExceeded**”类别以接收通知。

您可以指定与向您或其他用户发送通知的方式和时间相关的各种参数。选择首选的通信方式（例如，电子邮件、Slack、PagerDuty 和 ServiceNow 通知），然后定义通知的收件人。

有关如何设置配置文件和发送通知的更多信息，请参阅配置通知。

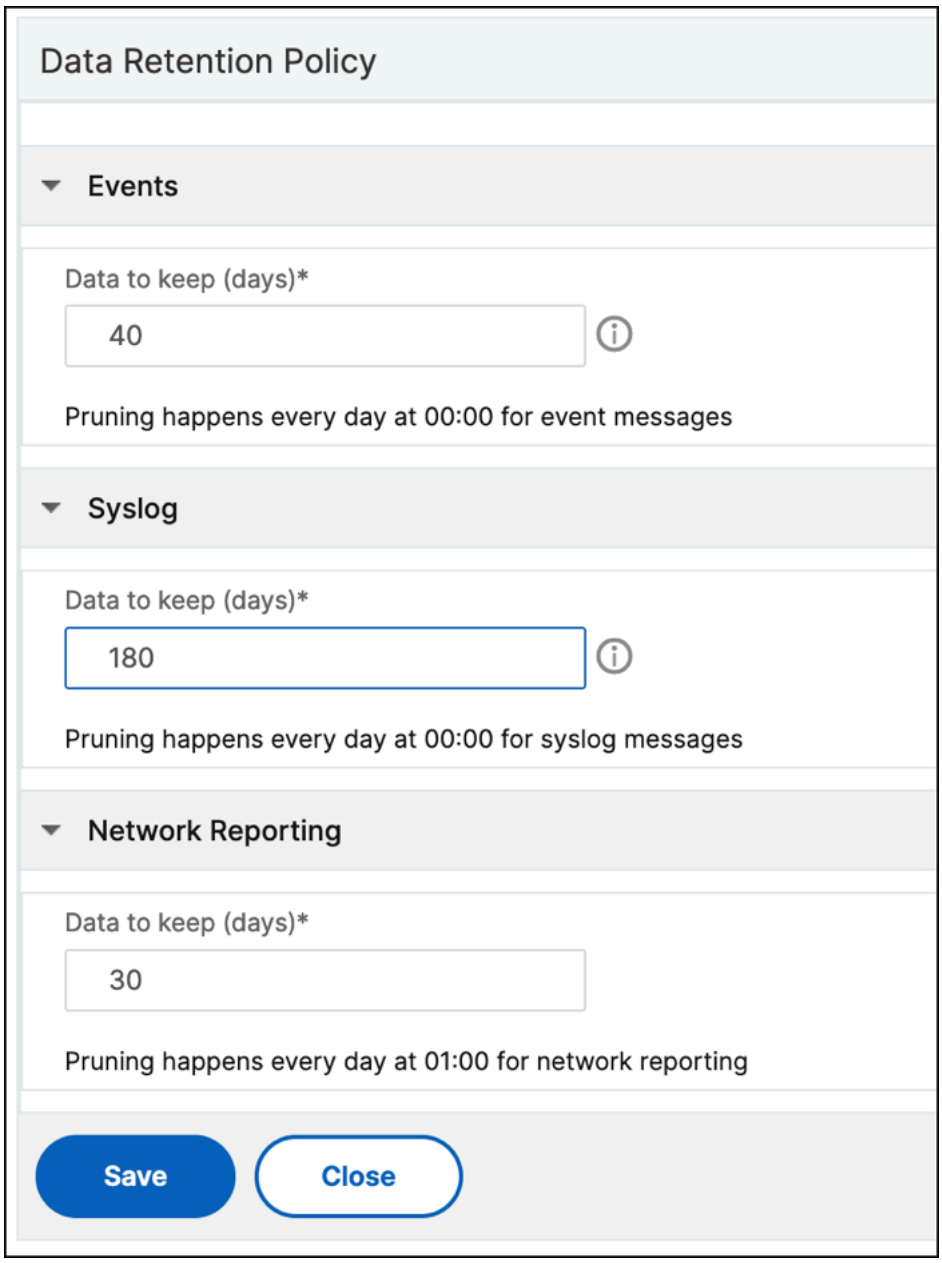
数据保留策略

January 29, 2024

您可以在 NetScaler 控制台中访问特定时间段内的系统事件、系统日志消息和网络报告数据。

1. 导航到设置 **>** 数据存储管理 **>** 数据保留策略以配置数据保留。
2. 单击“编辑”按钮。
3. 为以下每个选项输入您希望在 NetScaler 控制台中保留数据的天数：

选项	说明
事件	使您能够将存储在 NetScaler 控制台中的事件消息限制为 40 天。保留策略到期后，这些事件将从 NetScaler 控制台中删除。清除的事件在一天后被删除。
Syslog	使您能够将存储在数据库中的 syslog 数据量限制为最多 180 天。
网络报告	使您能够将存储在 NetScaler 控制台中的网络报告数据限制为 30 天。



重要：

您无法使用 Express 帐户编辑数据保留政策。

当您的帐户转换为 Express 帐户时，NetScaler 控制台最多可保留 500 MB 的存储数据或一天的数据，以较小者为准。有关更多信息，请参见 使用 Express 帐户管理 NetScaler 控制台资源。

配置和查看系统警报

May 9, 2024

您可以启用和配置一组警报来监视 NetScaler 控制台服务器的运行状况。您必须配置系统警报，以确保您了解任何关键或主要的系统问题。

例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。对于有些警报类别（例如 cpuUsageHigh 或 memoryUsageHigh），您可以为每项设置阈值并定义严重性（例如 “Critical”（严重）或 “Major”（重大））。对于有些类别（例如 inventoryFailed 或 loginFailure），只能定义严重性。当某个警报类别（例如，memoryUsageHigh）的阈值被突破时，或者当发生与该警报类别对应的事件（例如 loginFailure）时，系统会记录一条消息，您可以将该消息作为 syslog 消息查看。可以进一步设置通知以接收对应于警报设置的电子邮件或 SMS。

可以分配或修改警报的严重性。您可以分配的严重性级别为 “严重”、“严重”、“次要”、“警告” 和 “信息”。

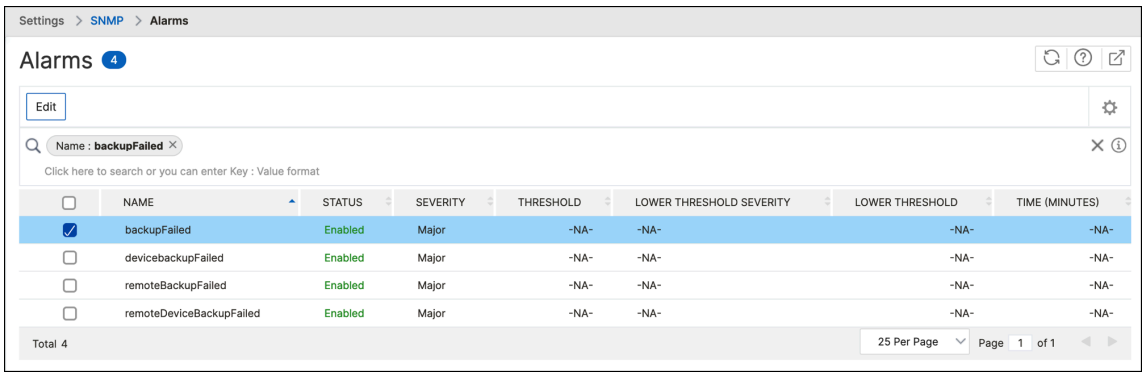
配置警报

假设您要监视失败的备份尝试。您可以启用 backupFailed 警报并为其分配严重性，例如 “主要”。每当 NetScaler 控制台尝试备份系统文件以及尝试失败时，都会触发警报。您可以在 NetScaler 控制台日志消息页面上查看该消息，也可以通过电子邮件或短信获取通知。

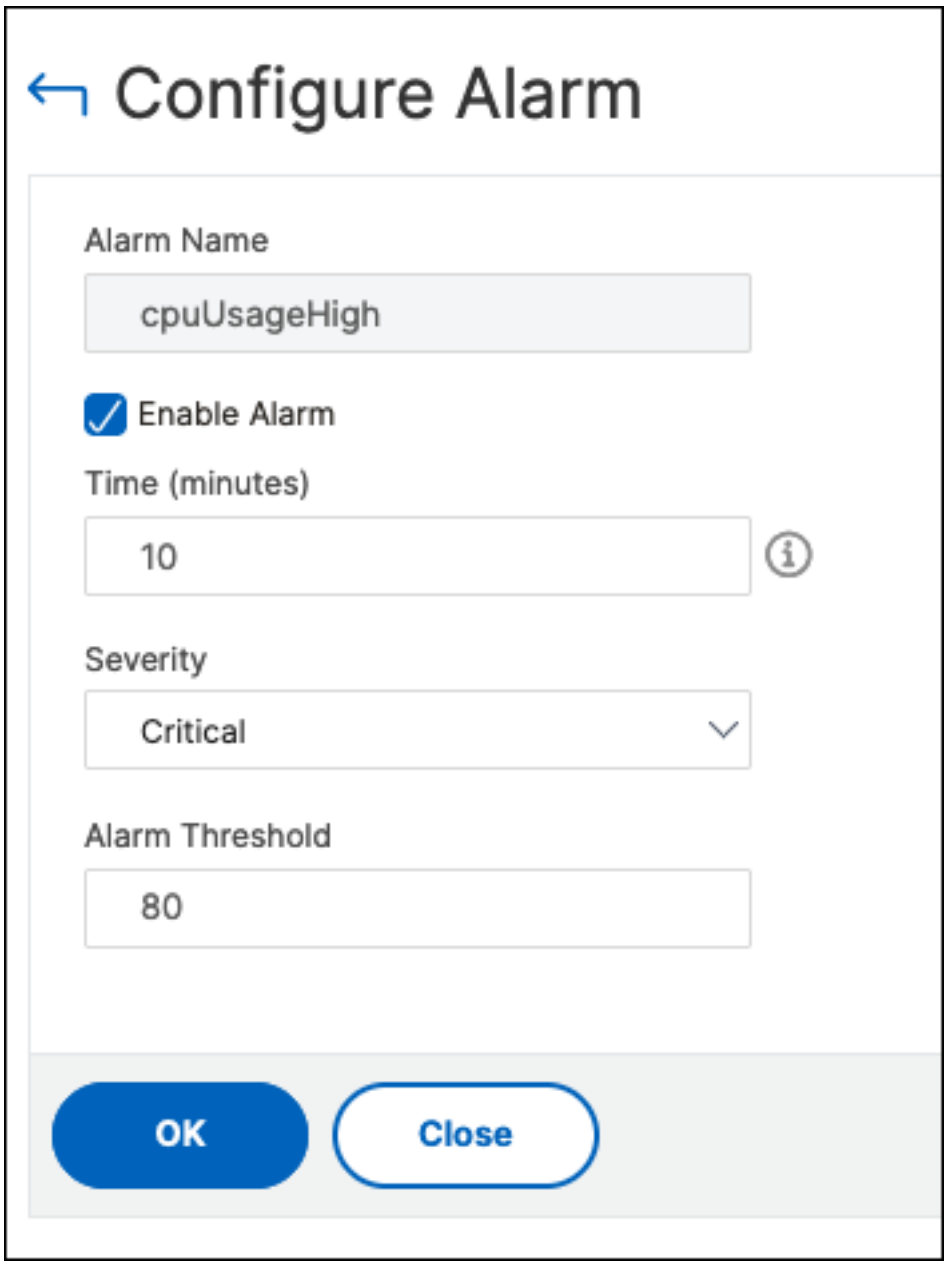
要配置警报，必须选择 backupFailed 警报并将严重性级别指定为 “主要”。默认情况下，启用警报。

要使用 NetScaler 控制台配置和查看系统警报，请执行以下操作：

1. 导航到设置 **> SNMP**。点击右上角的警报。



2. 选择要配置的警报（例如，cpuUsageHigh），然后单击 “编辑” 以修改其设置。



3. 在“配置警报”页面中，选择“启用警报”以创建警报，然后指定以下内容：

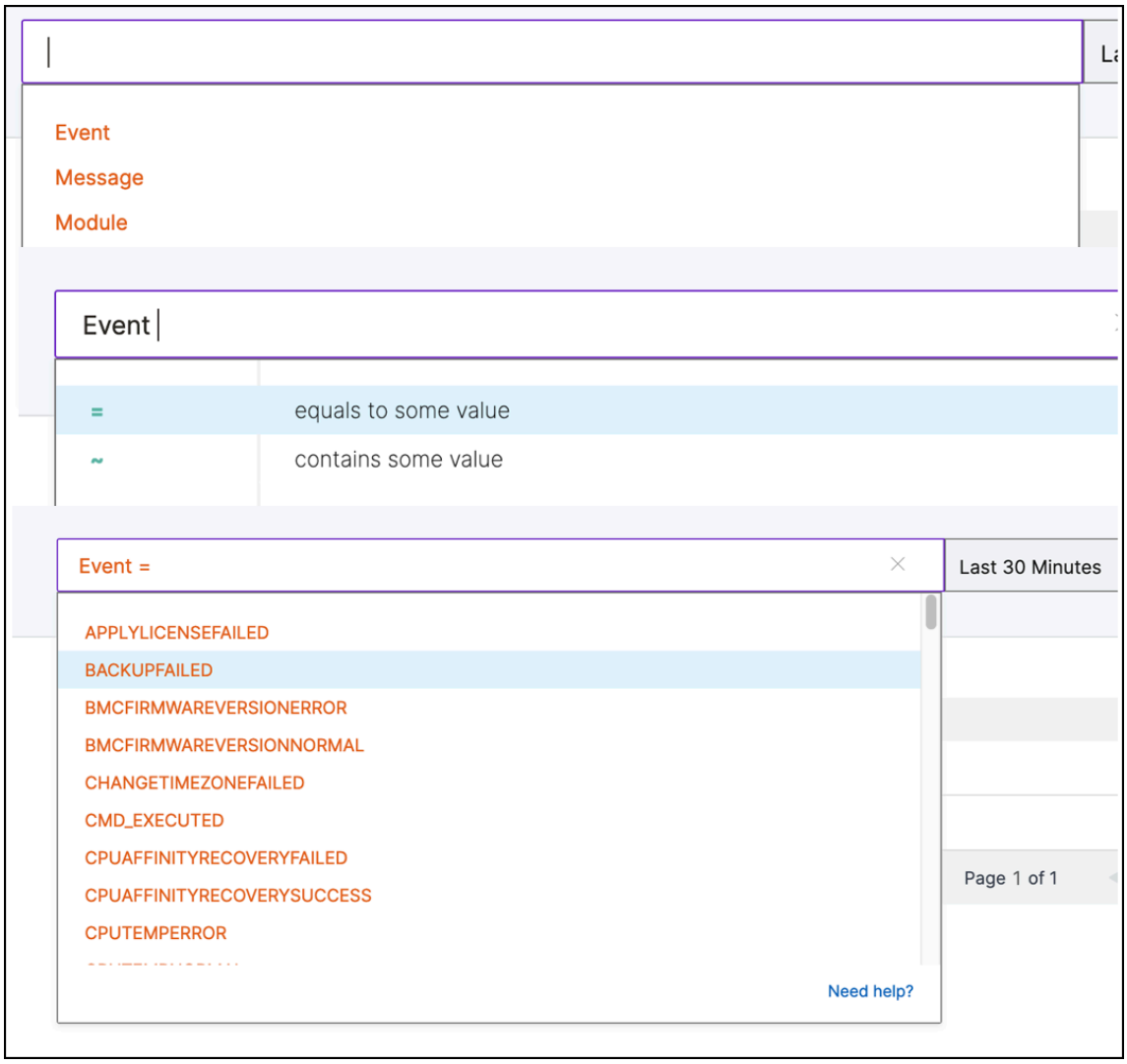
   - 时间。键入您要触发警报的时间（以分钟为单位）。
   - 严重程度。选择严重性级别。
   - 警报阈值。输入应触发警报和向您发送警报的值。

   单击确定。

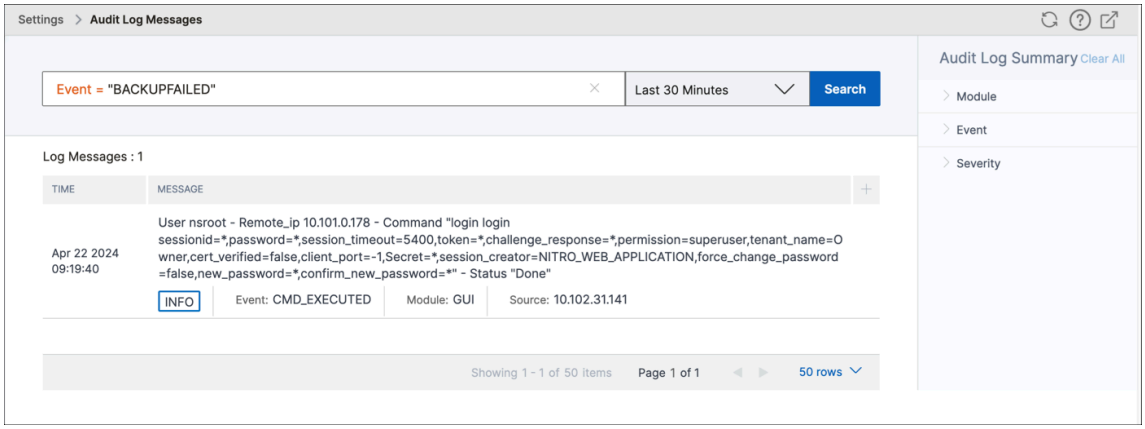
> 注意：
>
> 您无法为某些警报设置阈值，例如 backupFailed。触发警报后，可以查看以 syslog 消息形式存在的生成事件。

要查看警报生成的事件（例如，backupFailed），请执行以下操作：

1. 导航到“设置”>“审核日志消息”。
2. 在搜索字段中，选择警报的类型。在此示例中，选择“事件”、**=**（等于某个值），然后选择 **BACKUPFAILED**。



显示为备份失败而生成的事件。



您还可以将通知设置为在触发警报时接收电子邮件或 SMS（短消息服务）文本。

为磁盘利用率警报添加阈值限制

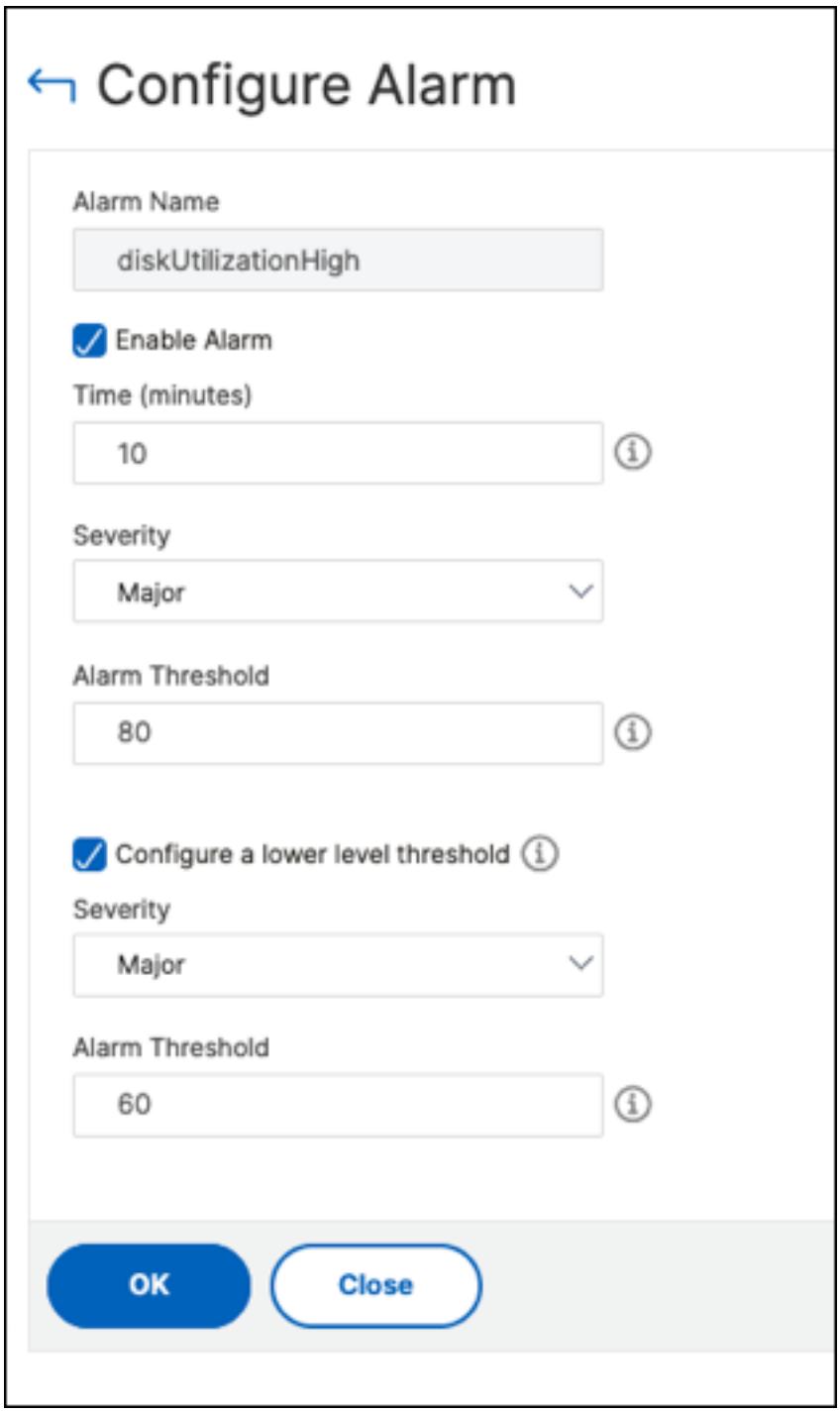
当 NetScaler 控制台服务器上使用的磁盘空间量超过预定义的阈值时，就会触发磁盘使用率警报。

作为管理员，当您收到警报时，您可以选择删除不必要的数据或分配额外的存储资源，以防止服务中断或性能下降。

自 14.1 内部版本 25x 开始，您还可以为磁盘利用率警报添加较低级别的阈值。使用此阈值，您可以设置较低级别的限制，以便在突破阈值上限之前接收警报。

要配置较低级别的阈值，请执行以下操作：

1. 导航到“设置”**>**“**SNMP**”**>**“警报”，然后在搜索字段中输入 diskUtilizationHigh 以查看磁盘利用率警报。
2. 选择警报，然后单击“编辑”。
3. 在配置警报页面中，选择配置较低级别的阈值。输入较低级别的阈值限制。



例如，如果您将较低的磁盘利用率阈值设置为 60，将上限阈值设置为 80，则当磁盘使用量超过磁盘容量的 60% 时，您会收到警报。此设置允许您在磁盘利用率达到 80% 之前采取纠正措施。

可观测性集成

July 17, 2024

由于现代应用程序越来越复杂，管理员在以下方面面临挑战：

- 监视和故障排除应用程序。
- 深入了解基础架构和应用程序的行为。

可观测性通过提供对整个基础设施的这些见解来弥合这一差距。使用 NetScaler 控制台中的可观测性集成功能，您可以：

- 将 NetScaler 控制台与 Splunk 集成。
- 将 NetScaler 控制台与 New Relic 集成。
- 将 NetScaler 控制台与 Microsoft Sentinel 集成
- 配置 NetScaler 实例，使用默认架构将见解导出到 Prometheus。

与 **Splunk** 集成

July 17, 2024

现在，您可以将 NetScaler 控制台与 Splunk 集成，以查看以下方面的分析：

- WAF 违规行为
- 机器人违规行为
- SSL 证书见解
- Gateway Insight

Splunk 插件使您能够：

- 合并所有其他外部数据源。
- 集中提供更高的分析可见性。

NetScaler 控制台收集 Bot、WAF、SSL 事件，并定期向 Splunk 发送事件。Splunk 通用信息模型 (CIM) 插件将事件转换为 CIM 兼容数据。作为管理员，您可以使用与 CIM 兼容的数据在 Splunk 控制板中查看事件。

要成功集成，您必须：

- 配置 Splunk 以接收来自 NetScaler 控制台的数据

- 配置 NetScaler 控制台以将数据导出到 Splunk
- 在 Splunk 中查看控制板

配置 **Splunk** 以接收来自 **NetScaler** 控制台的数据

在 Splunk 中，您必须：

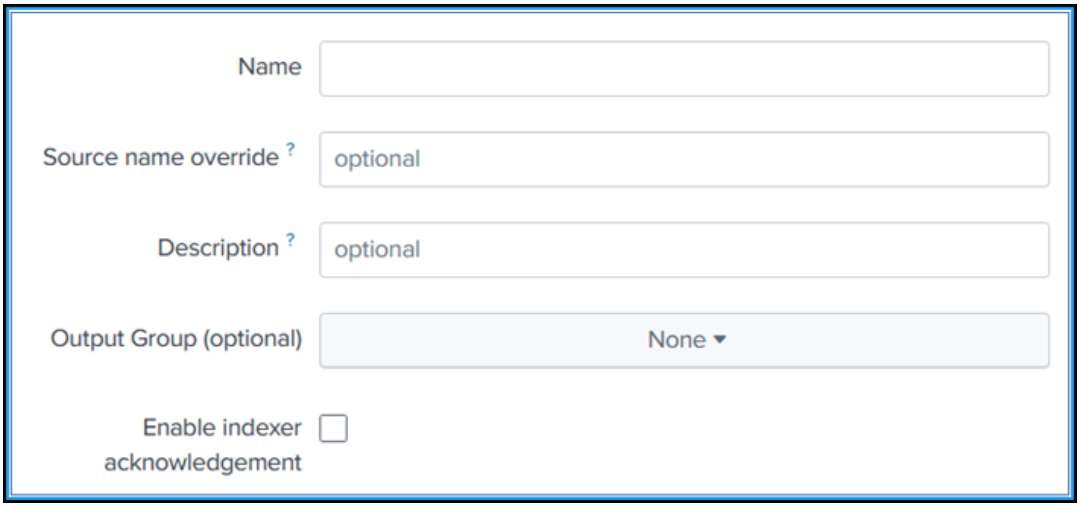
1. 设置 Splunk HTTP 事件收集器端点并生成令牌
2. 安装 Splunk 通用信息模型 (CIM) 插件
3. 安装 CIM 标准化器（仅适用于 WAF 和机器人见解）
4. 在 Splunk 中准备一个示例控制板

设置 **Splunk HTTP** 事件收集器端点并生成令牌

您必须先在 Splunk 中设置 HTTP 事件收集器。此设置允许在 NetScaler 控制台和 Splunk 之间进行集成，以发送 WAF 或 Bot 数据。接下来，您必须在 Splunk 中生成一个令牌以：

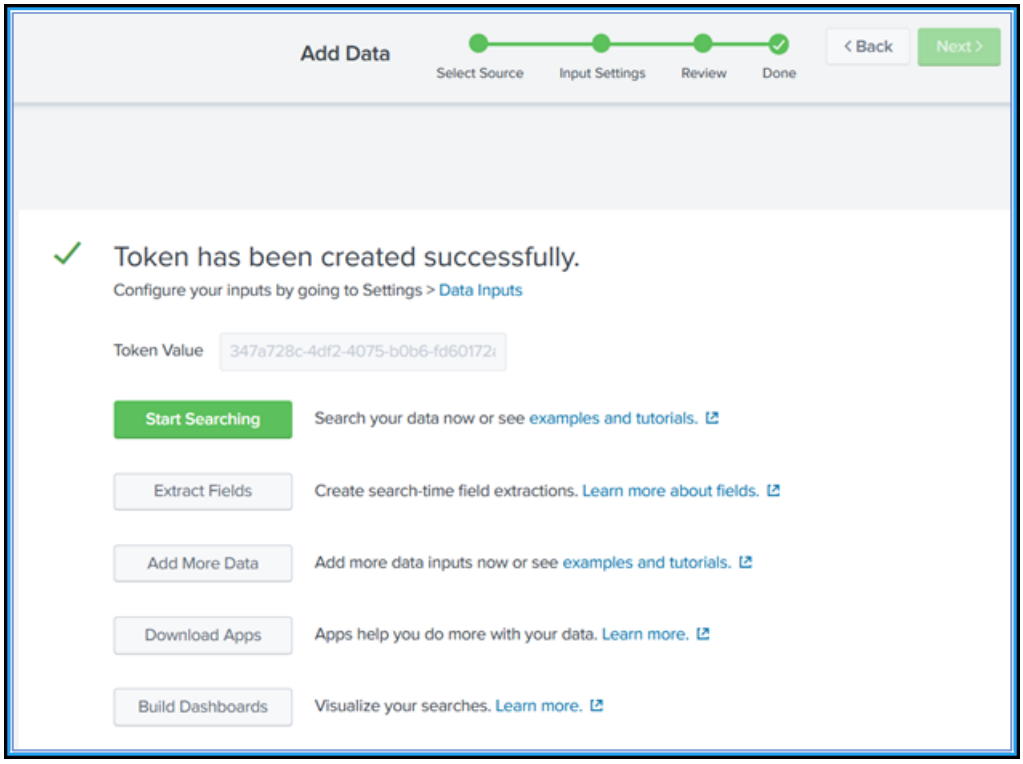
- 启用 NetScaler 控制台和 Splunk 之间的身份验证。
- 通过事件收集器端点接收数据。

1. 登录 Splunk。
2. 导航到“设置”**>**“数据输入”**>**“**HTTP** 事件收集器”，然后单击“新增”。
3. 指定以下参数：
    a) 名称：指定您选择的名称。
    b) 源名称覆盖（可选）：如果设置一个值，它将覆盖 HTTP 事件收集器的源值。
    c) 描述（可选）：指定描述。
    d) 输出组（可选）：默认情况下，此选项被选为无。
    e) 启用索引器确认：NetScaler 控制台不支持此选项。我们建议不要选择此选项。



4. 单击下一步。
5. 或者，您可以在“输入设置”页面中设置其他输入参数。
6. 单击“审阅”以验证参赛作品，然后单击“提交”。

   生成令牌。在 NetScaler 控制台中添加详细信息时，必须使用此令牌。

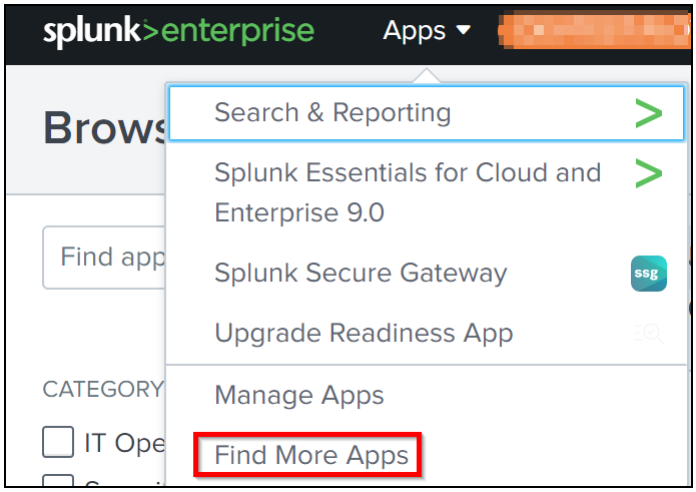


安装 **Splunk** 通用信息模型

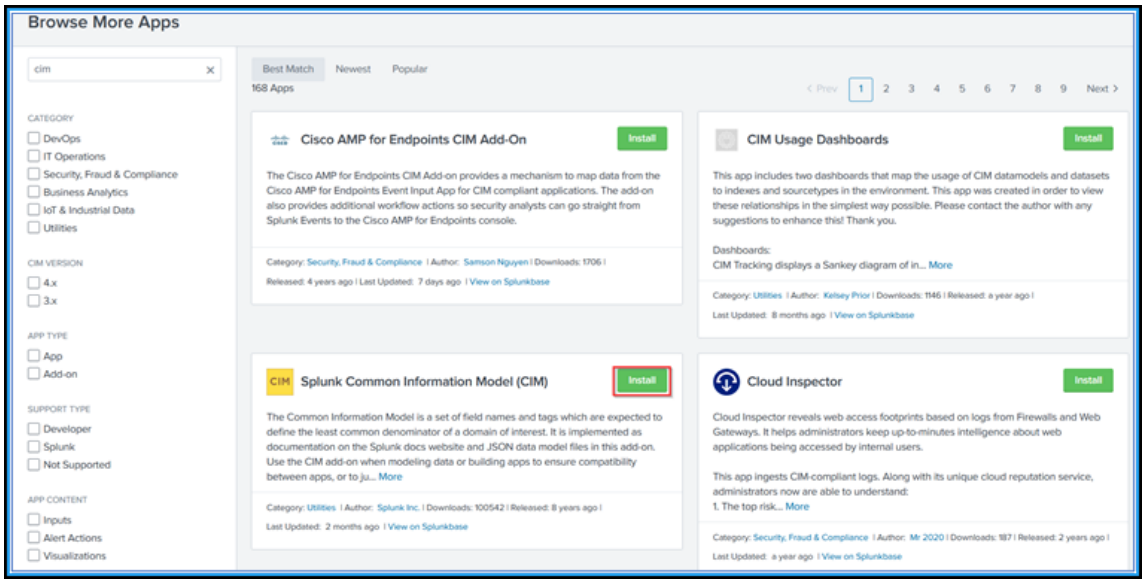
在 Splunk 中，您必须安装 Splunk CIM 附加组件。此插件可确保从 NetScaler 控制台接收的数据对采集的数据进行标准化处理，并使用相同的字段名称和事件标签来匹配通用标准，用于等效事件。

> 注意
>
> 如果您已经安装了 Splunk CIM 附加组件，则可以忽略此步骤。

1. 登录 Splunk。
2. 导航到 应用程序 **>** 查找更多应用程序。



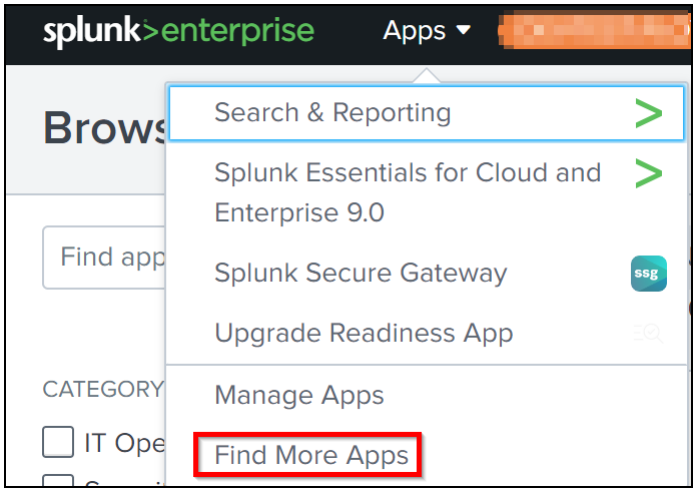
3. 在搜索栏中键入 **CIM** ，然后按 **Enter** 获取 **Splunk** 通用信息模型 **(CIM)** 插件，然后单击“安装”。



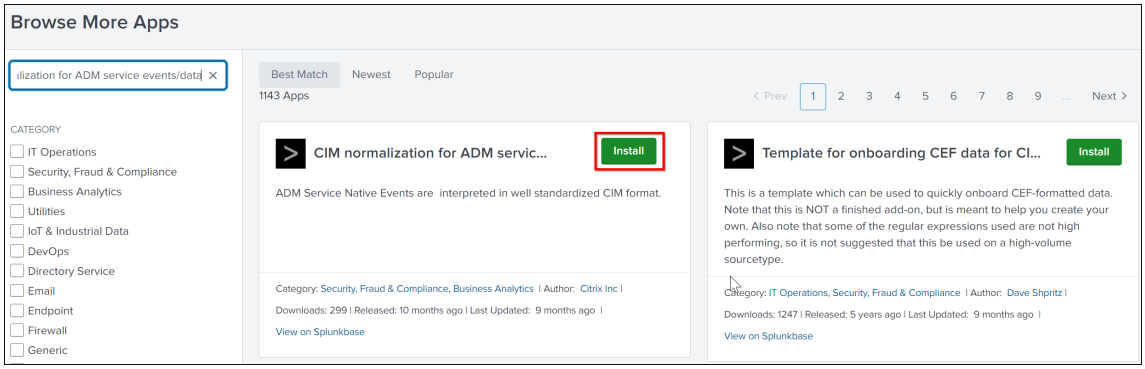
安装 **CIM** 标准化器

CIM 标准化器是一个附加插件，您必须安装该插件才能在 Splunk 中查看 WAF 和机器人见解。

1. 在 Splunk 门户中，导航到“应用程序” > “查找更多应用程序”。



2. 在搜索栏中键入 **ADM** 服务事件/数据的 **CIM** 标准化，然后按 **Enter** 获取插件，然后单击“安装”。



在 **Splunk** 中准备一个示例控制板

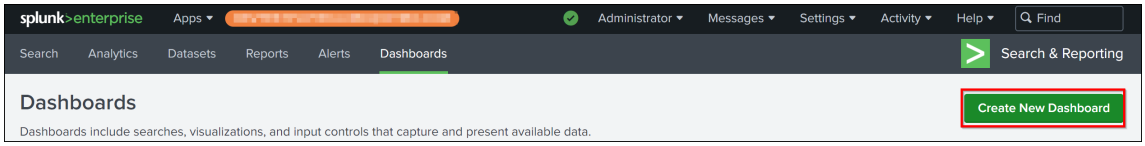
安装 Splunk CIM 后，必须使用 WAF 和 Bot 模板以及 SSL 证书见解准备示例控制板。您可以下载控制板模板 (`.tgz`) 文件，使用任何编辑器（例如，记事本）复制其内容，并通过在 Splunk 中粘贴数据来创建控制板。

> 注意：
>
> 以下创建示例控制板的步骤适用于 WAF 和 Bot 以及 SSL 证书见解。必须使用所需的 `json` 文件。

1. 登录 Citrix 下载页面，下载可 观测性集成下提供的示例控制板。
2. 提取文件，使用任意编辑器打开 `json` 文件，然后从文件中复制数据。

> 注意：
>
> 解压缩后，您会得到两个 `json` 文件。使用 `adm_splunk_security_violations.json` 创建 WAF 和 Bot 示例控制板，使用 `adm_splunk_ssl_certificate.json` 创建 SSL 证书洞察示例控制板。

3. 在 Splunk 门户中，导航到“搜索和报告” **>** “控制板”，然后单击“创建新控制板”。



4. 在“创建新控制板”页面中，指定以下参数：

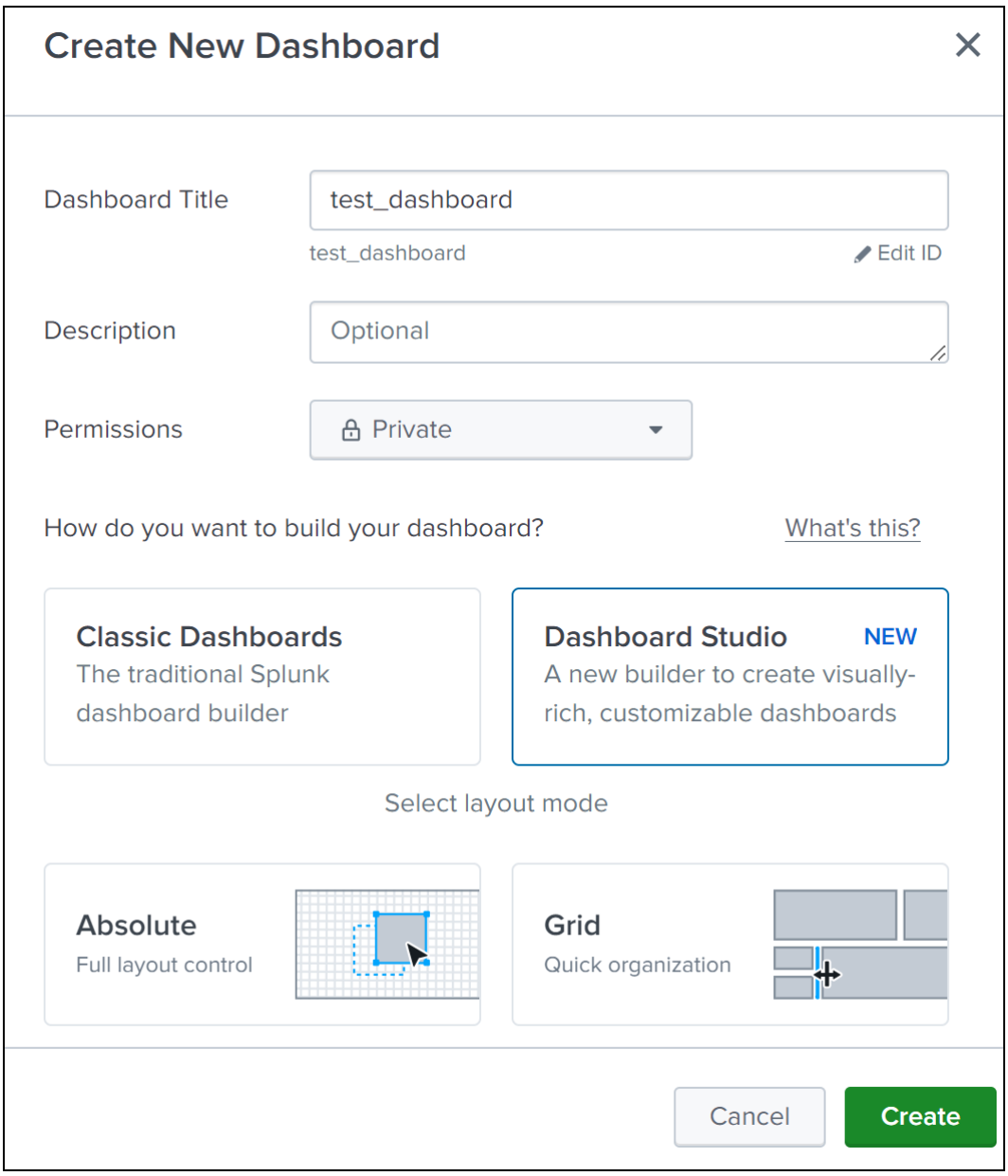
   a) 控制板标题 -提供您选择的标题。

   b) 说明 -（可选）您可以提供描述以供参考。

   c) 权限 -根据您的要求选择“专用”或“在应用程序中共享”。

   d) 选择“控制板 **Studio**”。

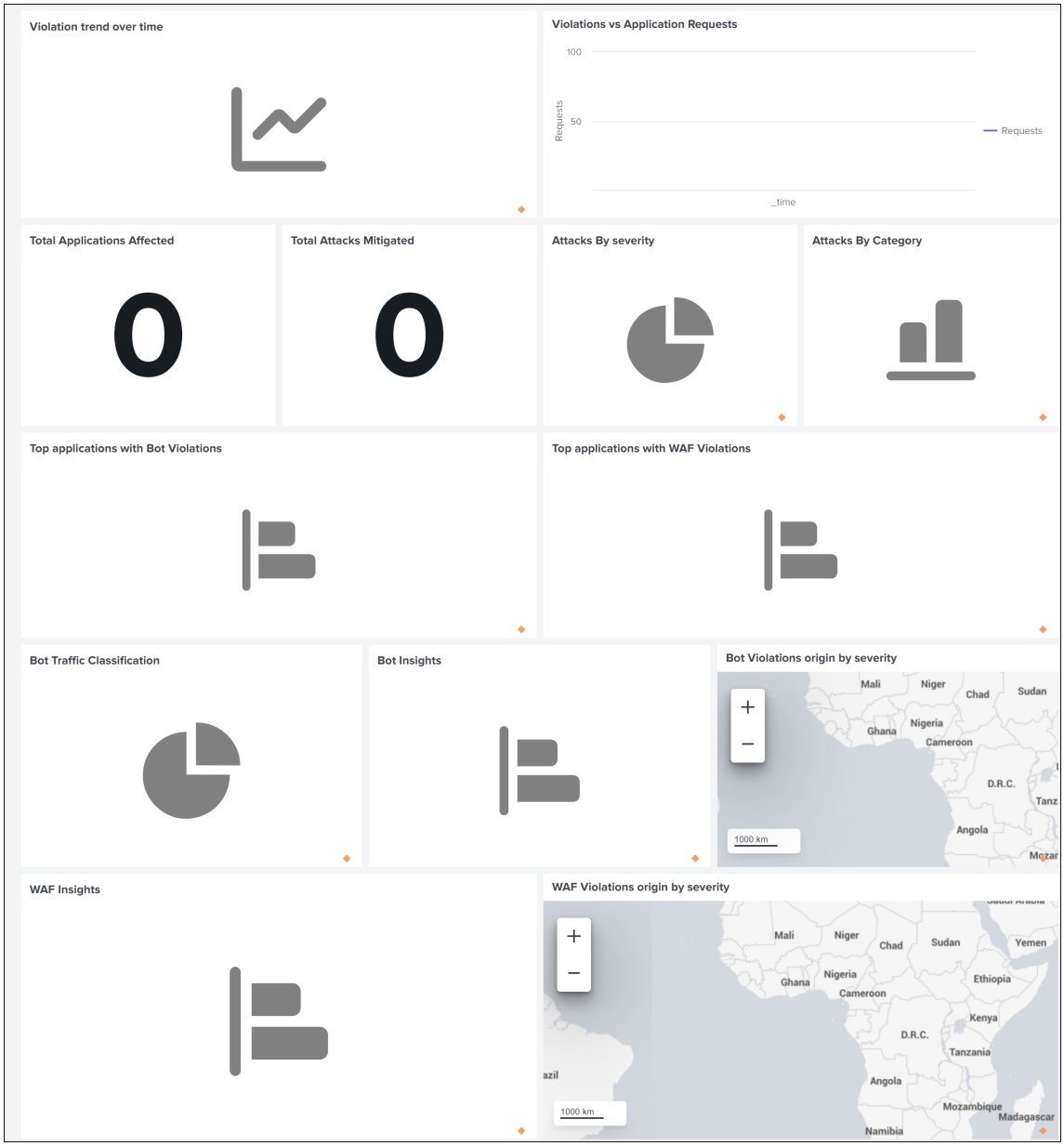
   e) 选择任意一种布局（绝对或网格），然后单击“创建”。



单击“创建”后，从布局中选择“源”图标。

5. 删除现有数据，粘贴您在步骤 2 中复制的数据，然后单击“返回”。
6. 单击保存。

   您可以在 Splunk 中查看以下示例控制板。



配置 **NetScaler** 控制台以将数据导出到 **Splunk**

现在，您已经在 Splunk 中准备好一切了。最后一步是通过创建订阅并添加令牌来配置 NetScaler 控制台。

完成以下步骤后，您可以在 Splunk 中查看更新后的控制面板，该控制面板目前在 NetScaler 控制台中可用：

1. 登录到 NetScaler 控制台。
2. 导航到“设置” **>** “可观测性集成”。
3. 在“集成”页面中，单击“添加”。
4. 在“创建订阅”页面中，指定以下详细信息：

a) 在“订阅名称”字段中指定您选择的名称。

b) 选择 **NetScaler** 控制台作为源，然后单击“下一步”。

c) 选择 **Splunk**，然后单击“配置”。在“配置端点”页面中：

i. 端点 **URL** - 指定 Splunk 端点详细信息。终点必须采用以下 https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event 格式。

> 注意：
>
> 出于安全考虑，建议使用 HTTPS。

- **SPLUNK_PUBLIC_IP** —为 Splunk 配置的有效 IP 地址。
- **SPLUNK_HEC_PORT** —表示您在 HTTP 事件端点配置期间指定的端口号。默认端口号为 8088。
- 服务/收集器/事件—表示 HEC 应用程序的路径。

ii. 身份验证令牌 -从 Splunk 复制并粘贴身份验证令牌。

iii. 单击 **Submit**（提交）。

d) 单击下一步。

e) 单击“添加见解”，在“选择功能”选项卡中，您可以选择要导出的功能，然后单击“添加选定功能”。

f) 单击下一步。

g) 在“选择实例”选项卡中，可以选择“选择所有实例”或“自定义选择”，然后单击“下一步”。

- 选择所有实例 -将数据从所有 NetScaler 实例导出到 Splunk。
- 自定义选择 - 允许您从列表中选择 NetScaler 实例。如果您从列表中选择特定实例，则仅将数据从选定的 NetScaler 实例导出到 Splunk。

h) 单击 **Submit**（提交）。

> 注意：
>
> 在 NetScaler 控制台中检测到违规行为后，所选见解的数据会立即推送到 Splunk。

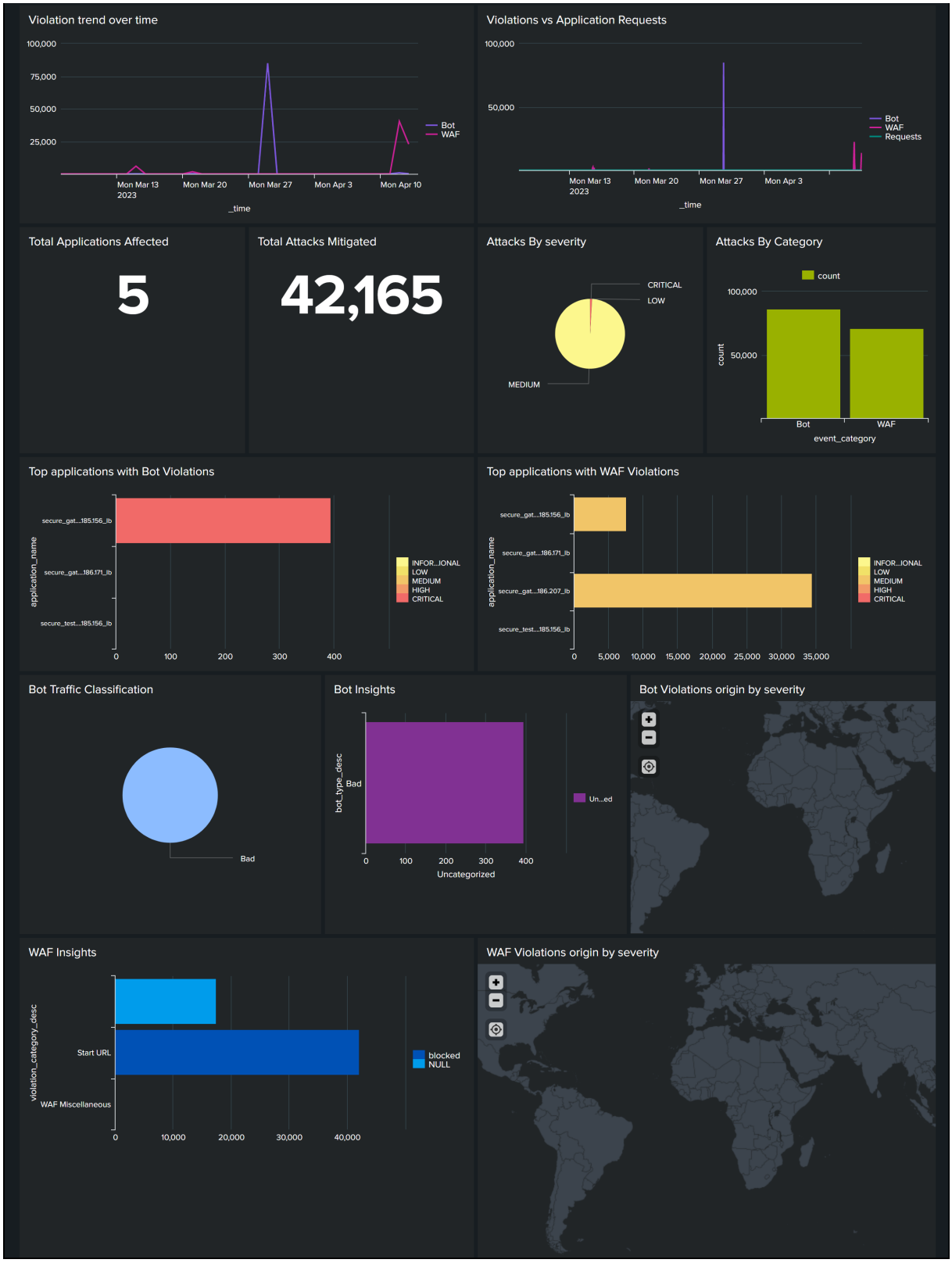
在 **Splunk** 中查看控制板

在 NetScaler 控制台中完成配置后，事件将显示在 Splunk 中。

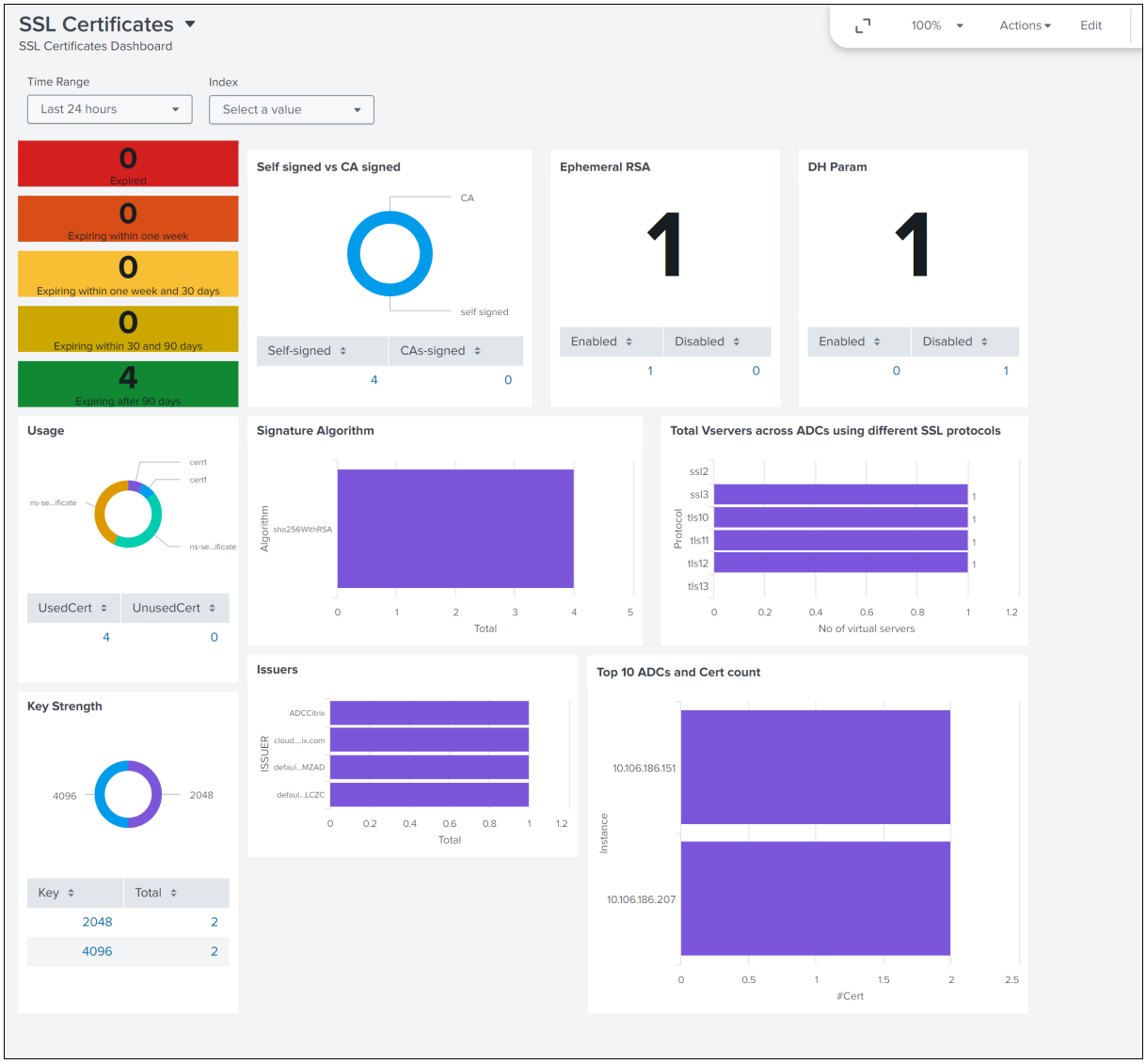
您无需任何其他步骤即可在 Splunk 中查看更新的控制板。

转到 Splunk 并单击您创建的控制板以查看更新的控制板。

以下是更新后的 WAF 和 Bot 控制板的示例：



以下控制板是更新后的 SSL 证书见解控制板的示例。



除了控制面板外，您还可以在创建订阅后在 Splunk 中查看数据

1. 在 Splunk 中，单击“搜索和报告”。
2. 在搜索栏中：
   - 键入 `sourcetype="bot"` 或 `sourcetype="waf"` 并从列表中选择持续时间以查看 bot/WAF 数据。
   - 在列表中键入 `sourcetype="ssl"` 并选择持续时间以查看 SSL 证书见解数据。
   - 键入 `sourcetype="gateway_insights"` 并从列表中选择持续时间以查看 Gateway Insight 数据。

与 **New Relic** 集成

July 17, 2024

现在，您可以将 NetScaler 控制台与 New Relic 集成，以便在 New Relic 控制面板中查看 WAF 和机器人违规行为的分析。通过这种集成，您可以：

- 在 New Relic 控制板中合并所有其他外部数据源。
- 集中查看分析情况。

NetScaler 控制台收集机器人和 WAF 事件，并根据您的选择实时或定期将它们发送到 New Relic。作为管理员，您还可以在 New Relic 控制板中查看机器人和 WAF 事件。

必备条件

要成功集成，您必须：

- 使用以下格式获取 New Relic 事件终端节点：

  ```
  https://insights-collector.newrelic.com/v1/accounts/<account_id>/events
  ```

  有关配置事件端点的更多信息，请参阅 New Relic 文档。

  有关获取帐户 ID 的更多信息，请参阅 New Relic 文档。
- 获取 New Relic 密钥。有关更多信息，请参阅 New Relic 文档。
- 在 NetScaler 控制台中添加关键细节

在 **NetScaler** 控制台中添加关键细节

生成令牌后，必须在 NetScaler 控制台中添加详细信息才能与 New Relic 集成。

1. 登录到 NetScaler 控制台。
2. 导航到“设置”**>**“可观测性集成”。
3. 在“集成”页面中，单击“添加”。
4. 在“创建订阅”页面中，指定以下详细信息：
   a) 在“订阅名称”字段中指定您选择的名称。
   b) 选择 **NetScaler** 控制台作为源，然后单击“下一步”。
   c) 选择“**New Relic**”，然后单击“配置”。在“配置端点”页面中：

i. 端点 **URL** —指定 New Relic 端点的详细信息。终点必须采用以下 `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` 格式。

> 注意
>
> 出于安全考虑，建议使用 HTTPS。

d) 身份验证令牌 - 复制并粘贴来自 New Relic 的身份验证令牌。

i. 单击 **Submit**（提交）。

e) 单击下一步。

f) 单击“添加见解”，在“选择功能”选项卡中，您可以选择要导出的功能，然后单击“添加选定功能”。

g) 单击下一步。

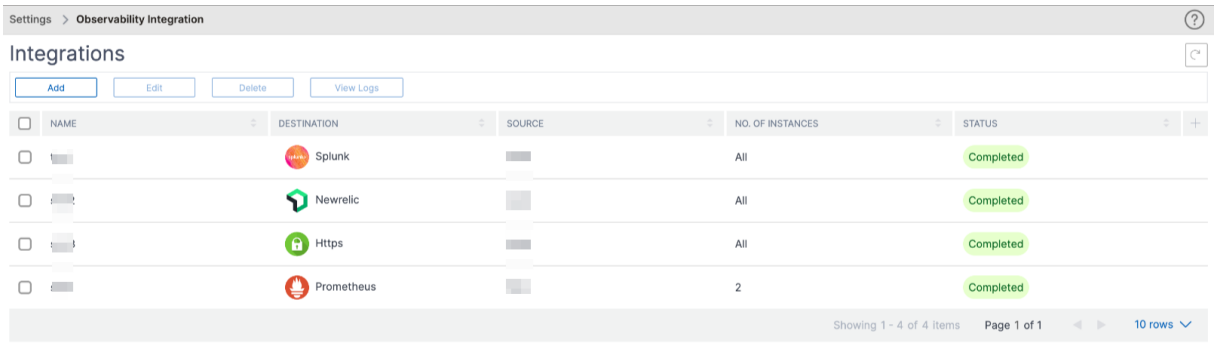
h) 在“选择实例”选项卡中，可以选择“选择所有实例”或“自定义选择”，然后单击“下一步”。

- 选择所有实例 -将数据从所有 NetScaler 实例导出到 New Relic。
- 自定义选择 - 允许您从列表中选择 NetScaler 实例。如果您从列表中选择特定实例，则仅将数据从选定的 NetScaler 实例导出到 New Relic。

i) 单击 **Submit**（提交）。

> 注意：
>
> - 在 NetScaler 控制台中检测到违规行为后，所选见解的数据会立即推送到 New Relic。

配置已完成。您可以在“订阅”页面中查看详细信息。

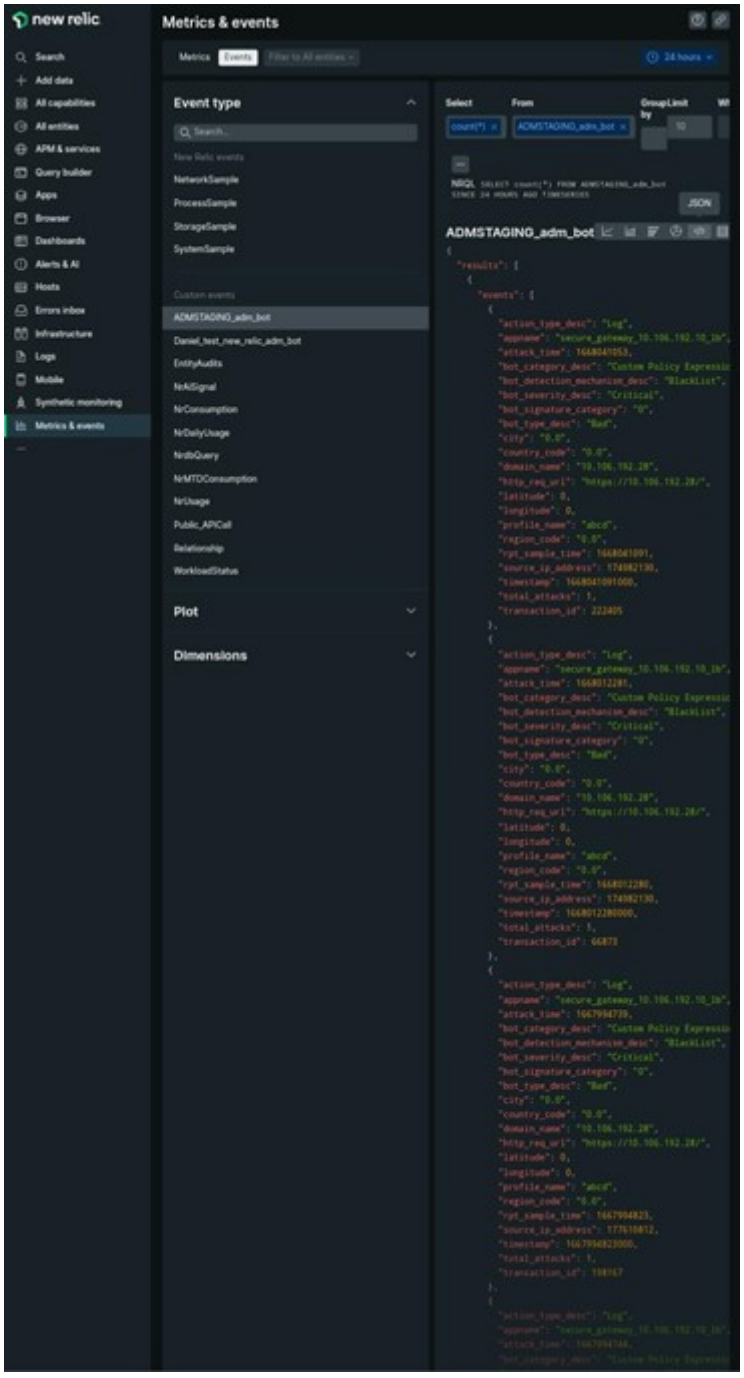


New Relic 控制板

在 New Relic 中导出事件后，您可以使用以下 JSON 格式在“指标和事件”下查看事件详细信息：

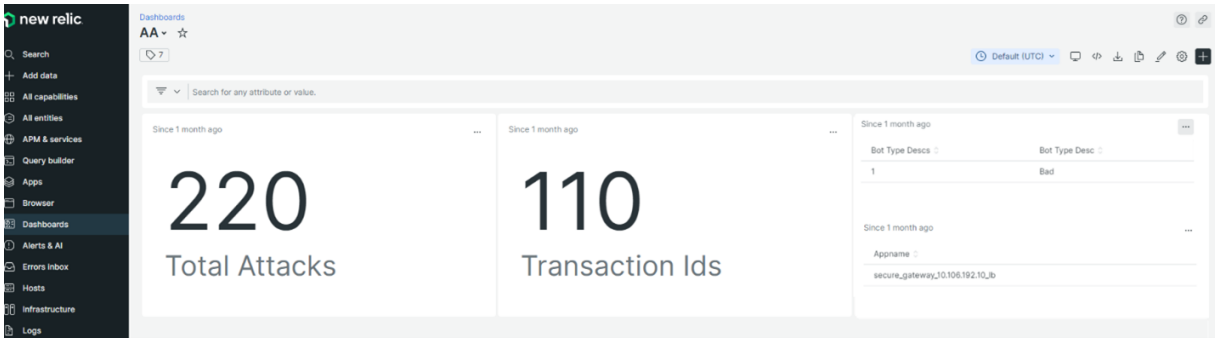
`<subsription_name>_adm_<event name>`，其中事件名称可以是机器人、WAF 等。

在以下示例中，ADMSTAGING 是 <subscription_name>，机器人是 <event_name>。



将 JSON 数据提取到 New Relic 控制板后，作为管理员，您可以使用 NRQL（New Relic Query Language），通过围绕提取的数据构建查询，根据您的选择创建包含分面和小部件的自定义控制板。有关详细信息，请参阅https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/

以下是使用 NRQL 创建的控制板示例：



要创建此控制板，需要进行以下查询：

- 组件 1：事件表中的传奇攻击总数

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- 组件 2：事件表中的唯一事务 ID

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days ago
  ```

- 组件 3：独特机器人类型总数及其数量

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <event_name> since 30 days ago
  ```

- 组件 4：看到机器人违规行为的唯一应用程序名称总数

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

与 **Microsoft Sentinel** 集成

September 2, 2024

您可以将 NetScaler 控制台与 Microsoft Sentinel 集成，将以下分析从 NetScaler 控制台导出到 Microsoft Sentinel：

- WAF 违规行为
- 机器人违规行为
- SSL 证书见解
- Gateway Insight

Microsoft Sentinel 提供集中式数据收集，可从应用程序、服务器等各种来源收集数据。作为管理员，您可以在 Microsoft Sentinel 中报告见解或违规行为后查看数据并做出决策。

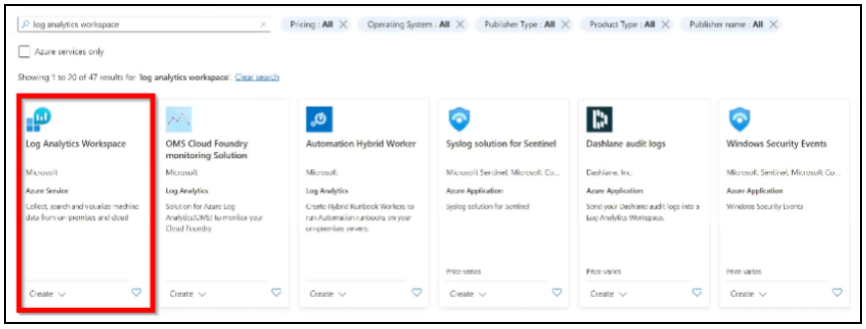
要成功集成，请确保您拥有有效的 Azure 订阅，然后按照每个部分下的步骤进行操作：

配置日志分析工作区

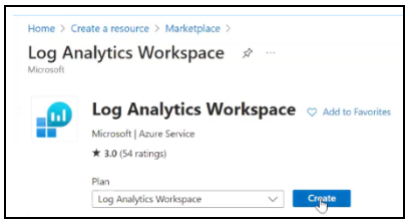
需要日志分析工作区来存储和分析收集的数据。

1. 登录到 Azure。
2. 单击 创建资源。

3. 在搜索栏中，键入日志分析工作区，然后单击“日志分析工作区”下的“创建”。



4. 在日志分析工作区主页上，单击“创建”。



5. 在创建日志分析工作区中：

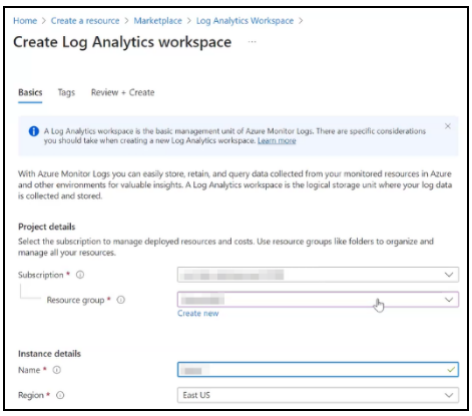
   a) 选择有效的订阅和资源组。

   > 注意：
   >
   > 如果您有权限，也可以单击“新建”来添加资源组。

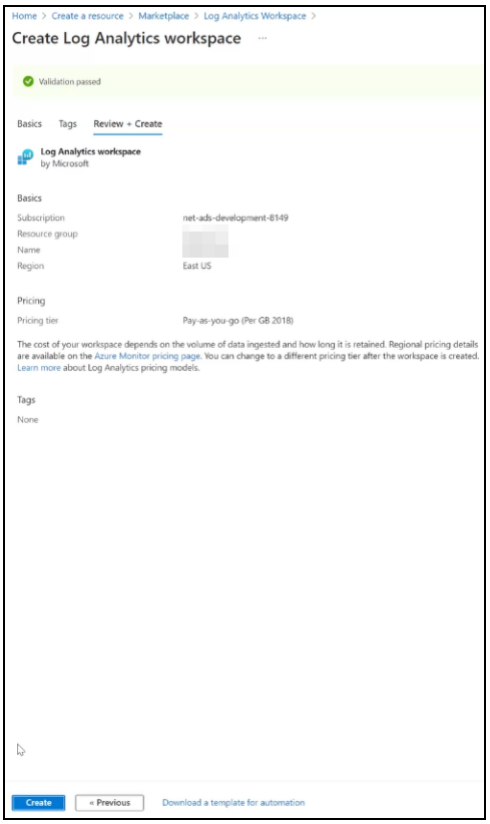
   b) 指定您选择的名称。

   c) 从列表中选择您所在的地区。

   d) 单击“查看 + 创建”。



e) 将显示验证通过消息。单击“创建”以部署工作区。



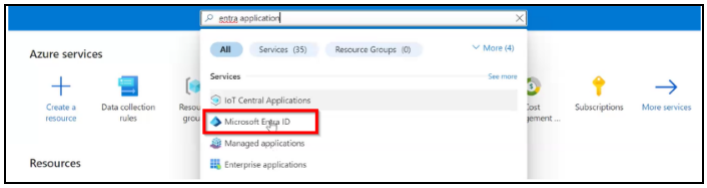
f) 您可以看到正在部署的消息。看到部署完成消息后，单击“转到资源”。

工作区已成功创建。

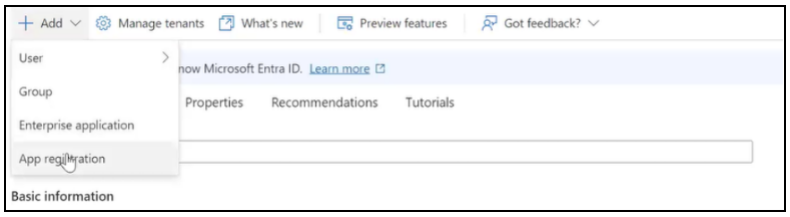
创建 **Microsoft Entra** 应用程序

必须创建与 Azure 订阅关联的 Entra 应用程序，才能代表日志分析工作区进行通信。创建应用程序后，还必须授予 **Microsoft Sentinel** 贡献者角色的权限。该应用程序还提供客户端 **ID**、租户 **ID** 和客户端密钥等详细信息。我们建议您记下这些细节。当您在 NetScaler 控制台中创建订阅以完成集成过程时，需要提供这些详细信息。

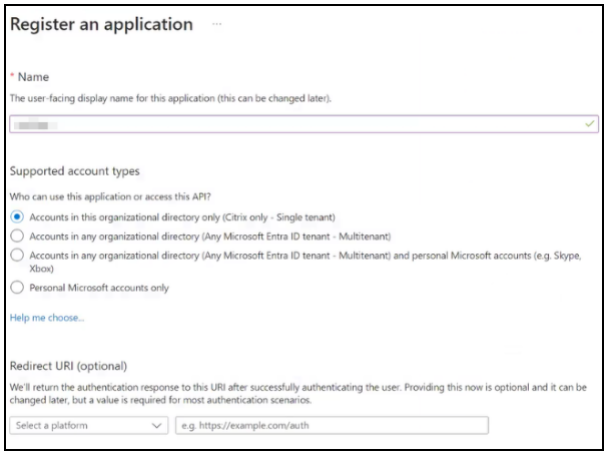
1. 在 Azure 门户中，在搜索栏中键入关键字。
2. 单击“**Microsoft Entra ID**”。



3. 单击“添加”，然后选择“应用程序注册”。

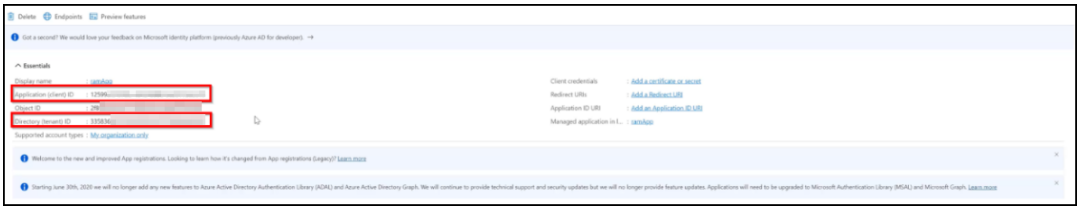


4. 为应用程序指定名称，在“支持的帐户类型”下选择“默认选项”，然后单击“注册”。



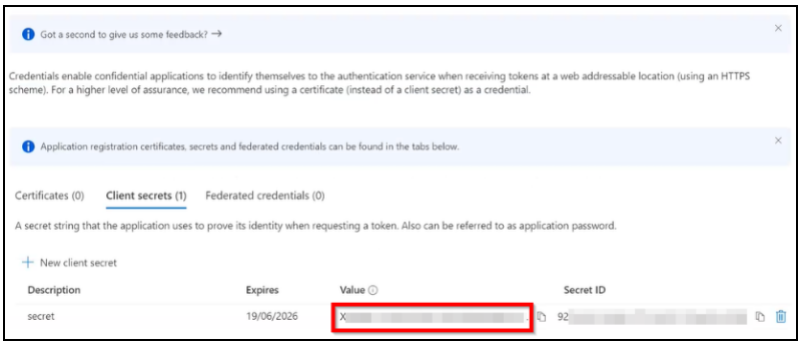
5. 注册应用程序后：

   a) 记下客户端 **ID** 和租户 **ID**。



b) 为您的应用程序创建密钥 ID。单击“证书和密钥”，然后在“客户端密钥”下，单击“新建客户端密钥”。提供描述和有效期，然后单击“添加”为您的应用程序创建密钥 ID。

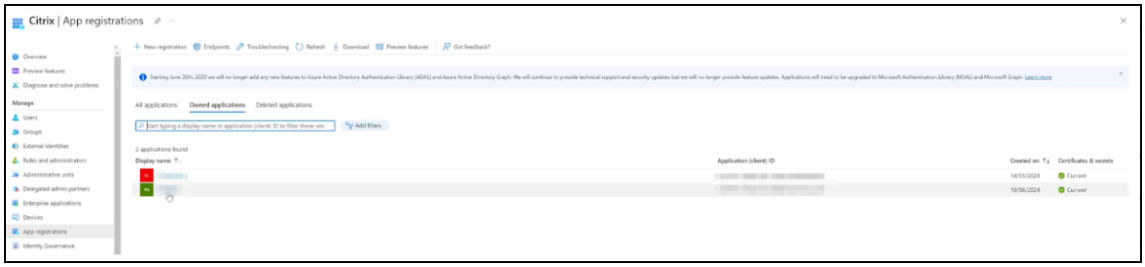
c) 将显示您的应用程序的详细信息。确保在创建密钥后立即记下“值”下显示的 ID。如果您导航到任何其他 GUI 选项，该值将被隐藏。



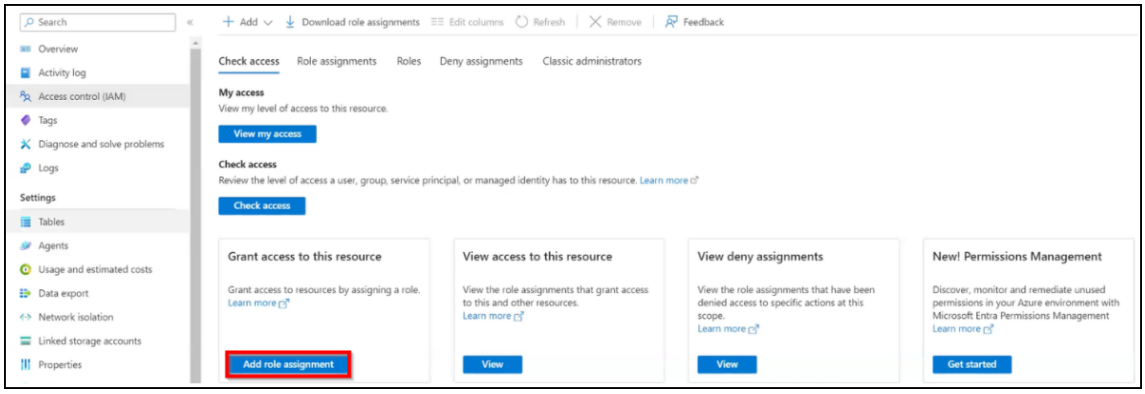
为 **Entra** 应用程序分配权限

您必须为应用程序分配 Microsoft Sentinel 贡献者角色。要授予权限，请：

1. 在 Azure 门户中导航到 Microsoft Entra ID。
2. 单击“应用程序注册”，然后选择您的应用程序。



3. 单击“访问控制 **(IAM)**”，然后单击“添加角色分配”。

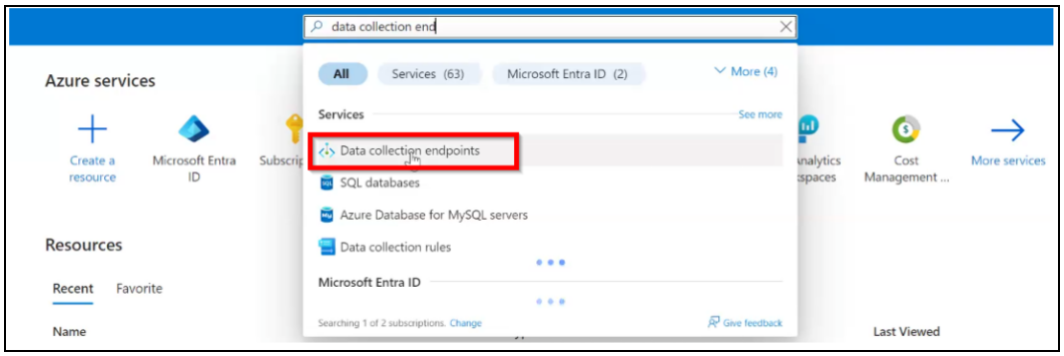


4. 在搜索栏中，键入关键字 sentinel，选择 **Microsoft Sentinel** 贡献者，然后单击“下一步”。
5. 在“成员”选项卡中，单击“选择成员”，然后选择您创建的 Entra 应用程序。
6. 单击 **Review + assign**（检查 + 分配）。

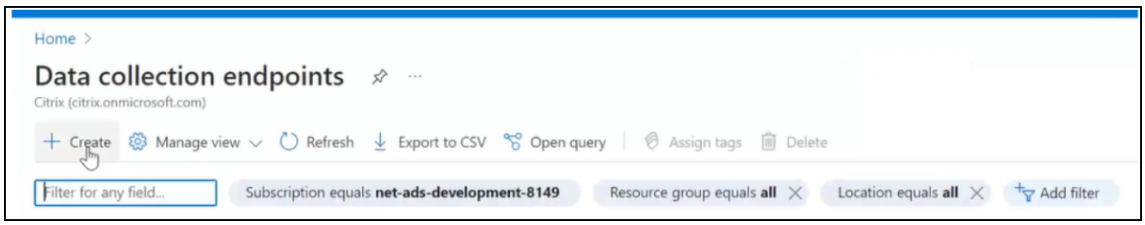
配置数据收集端点

必须创建数据收集端点才能获取端点 URL。当您在 NetScaler 控制台中创建订阅时，这是必需的。

1. 在 Azure 门户的 **Azure** 服务下，选择数据收集端点或在搜索栏中键入关键字。



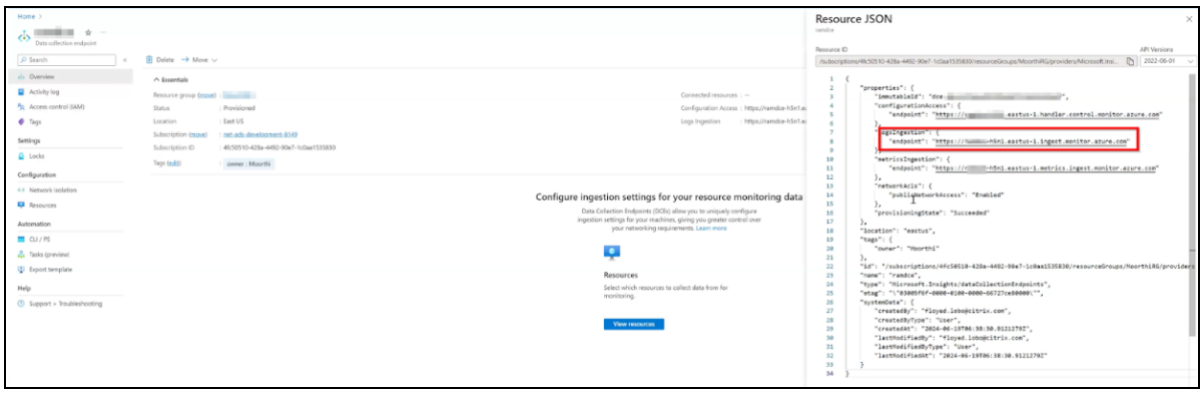
2. 在“数据收集端点”页面中单击“创建”。



3. 在创建数据收集端点中：
   a) 指定您选择的端点名称
   b) 选择订阅、资源组和区域。
   c) 单击“查看 + 创建”。

d) 看到验证通过的消息后，单击“创建”。

您必须记下端点 URL。在数据收集端点主页中，选择创建的终端节点，单击 **JSON** 视图，然后记下端点 ID。



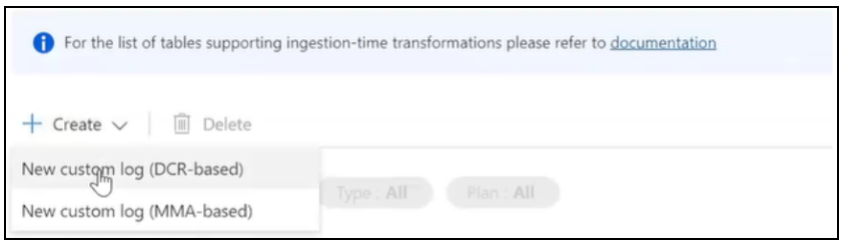
创建表以导出数据

对于要从 NetScaler 控制台导出到 Microsoft Sentinel 的每项见解，您必须创建一个表并提供 JSON 信息。您可以参考以下有关每项见解的表格要求的详细信息：

见解	所需的桌子总数
SSL 见解	3
WAF	1
机器人	1
Gateway Insight	5

对于每个工作区，您最多可以创建 10 个表。超过 10 个表，必须创建另一个工作区。

1. 在 Azure 门户中导航到您的工作区，然后单击“设置”下的“表”。
2. 单击“创建”，然后选择“新建自定义日志”（基于 **DCR**）



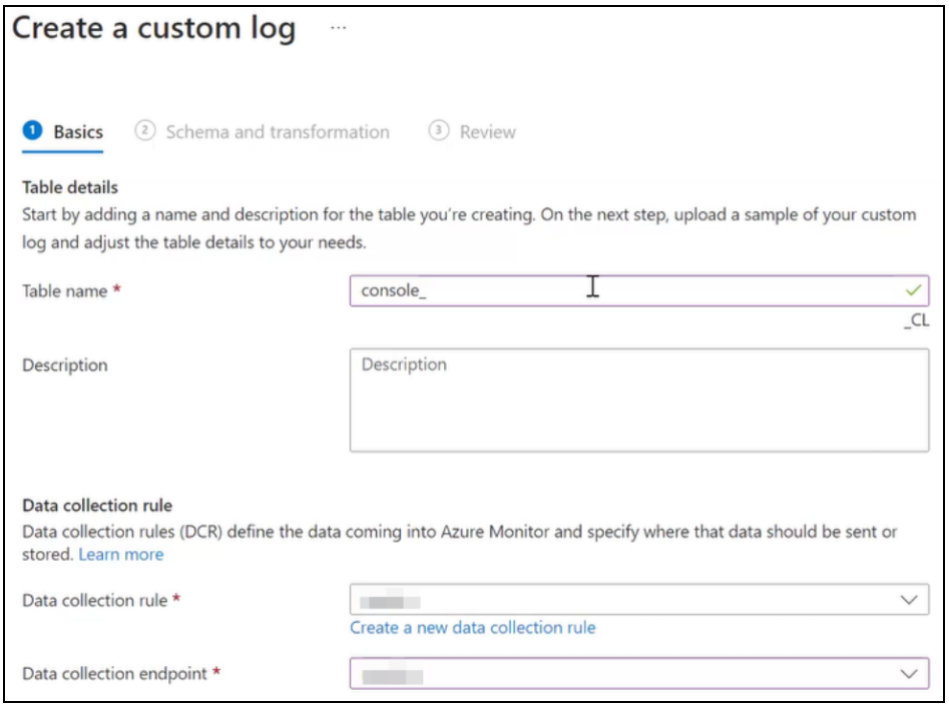
3. 在“创建自定义日志”中：

   a) 指定表名。表名必须采用 **console_insightname** 格式。例如：**console_ns_sslvserver**、**console_ns_ssl_certkey**。您可以参考步骤 4 来获取适用于每个见解的表名。

b) 提供描述以添加有关表名的更多信息。此为可选设置。

c) 创建新的数据收集规则并添加。

d) 从列表中选择数据收集端点。



e) 单击下一步。

4. 在架构和转换选项卡中，您必须为要导出的见解上载 JSON 示例日志。您可以为每个见解使用以下示例 JSON，并创建一个 JSON 文件进行上载：

见解	JSON	要使用的表名

见解	JSON	要使用的表名
SSL (1)	{ "id": "3eb05733-c326-493c-9aa0-f7db3a6b4277", "ns_ip_address": "10.106.186.141", "name": "zeta_192_168_110_250", "vsvr_ip_address": "", "vsvr_port": -1, "vsvr_type": "", "state": "", "partition_name": "", "display_name": "10.106.186.141", "poll_time": 1716539986, "managed": "f", "ssl2": "f", "ssl3": "t", "tls10": "t", "tls11": "t", "tls12": "t", "dh": "f", "ersa": "t", "sslprofile": "", "tls13": "f", "dhkeyexpsizelimit": "DISABLED", "pushenctriggertimeout": 1, "sessionticket": "", "includesubdomains": "f", "sessionticketkeyrefresh": "", "ssllogprofile": "", "serverauth": "", "ssltriggertimeout": 100, "ersacount": 0, "strictcachecks": "NO", "dhfile": "", "sessreuse": "ENABLED", "redirectportrewrite": "DISABLED", "	console_ns_sslvserver

见解	JSON	要使用的表名
SSL (2)	{ "id": "a6673ab2-0b59-47b9-b530-bc30fb2b937c", "ssl_certificate": "/nsconfig/ssl/ca-cert.pem", "ssl_key": "/nsconfig/ssl/ca-key.pem", "certkeypair_name": "athul-ca", "cert_format": "PEM", "days_to_expiry": 281, "ns_ip_address": "10.106.186.141", "status": "Valid", "device_name": "10.106.186.141", "file_location_path": "", "certificate_data": "", "key_data": "", "poll_time": 1717434335, "no_domain_check": "f", "version": 3, "serial_number": "7B34B6A6A1A79E0FF168242D7BCFF78F04C9EE66", "signature_algorithm": "sha256WithRSAEncryption", "issuer": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "valid_from": "Mar 12 08:51:11 2024 GMT", "valid_to": "Mar 12 08:51:11 2025 GMT", "subject": "C=IN,ST=KA,L=BAN,O=CIT,OU=ADM,CN=A", "public_key_algorithm": "rsaEncryption", "public_key_size": 4096, "	console_ns_ssl_certkey

见解	JSON	要使用的表名
SSL (3)	{ "id": "2baffd1a-7ed6-4035-91e8-ad3a3125bff4", "certkeypair_name": "cert1", "ns_ip_address": "10.106.186.127", "poll_time": 1715671567, "partition_name": "", "display_name": "10.106.186.127", "hostname": "", "entity_name": "secure_gateway", "entity_type": "sslvserver", "table_name": "ns_sslcertkey_binding"}	console_ns_sslcertkey_binding

见解	JSON	要使用的表名
WAF	[{ "ip_address": "10.106.185.156", "ctnsappname": "vserver_1", "severity": 2, "violation_type": 19, "violation_type_desc": "Start URL", "block_flags": 1, "transformed_flags": 0, "not_blocked_flags": 0, "country_code": "-NA-", "region_code": "-NA-", "city": "-NA-", "latitude": 200.0, "longitude": 200.0, "signature_category": "", "attack_category": 2, "attack_category_desc": "Broken Authentication and Session Management", "total_attacks": 1, "rpt_sample_time": 1704783773, "source_ip_address": 174766492, "attack_time": 1704783538, "profile_name": "appfw_cs_lb_prof", "session_id": "", "http_req_url": "https://10.106.192.54/csrf_ffc/ffc.html?field10=asfasd", "violation_name": "-NA-", "violation_value": "-NA-", "violation_location": 4, "violation_threat_index	console_af_threat_exporter_data_l2

见解	JSON	要使用的表名
机器人	{ "ip_address": "10.106.186.122", "ctnsappname": "secure_gateway", "bot_type": "2", "bot_type_desc": "Bad", "action_type": "6", "action_type_desc": "Log", "country_code": "0.0", "region_code": "0.0", "city": "0.0", "bot_severity": "0", "bot_severity_desc": "Critical", "latitude": "0", "longitude": "0", "bot_detection_mechanism": "6", "bot_detection_mechanism_desc": "BlackList", "bot_category": "0", "bot_category_desc": "Uncategorized", "source_ip_address": "174758625", "bot_signature_category": "Custom Policy Expression", "appname": "secure_gateway_10.106.186.122_lb", "backend_vserver": "", "backend_appname": "", "total_attacks": "2", "rpt_sample_time": "1718783216", "table_name": "af_bot_attack_details_l2"}	console_af_bot_attack_details_l2

见解	JSON	要使用的表名
Gateway Insight (1)	{ "adc_ip_address": "10.106.186.141", "auth_server": "", "client_ip": 174766732, "epa_method_type": 0, "error_count": 14, "error_details": "Invalid credentials passed", "error_type": 1, "gateway_name": "vpn_vserver_142_6", "req_url": "", "resource": "", "rpt_sample_time": 1713505215, "sso_method_type": 0, "sta_ip": "", "table_name": "af_vpn_error_details", "username": "John"}	console_af_vpn_error_details
Gateway Insight (2)	{ "adc_ip_address": "10.102.71.166", "display_name": "10.102.71.166", "gateway_name": "firsthop", "ip_address": "10.102.71.168", "rpt_sample_time": "1718812158", "state": "Up", "table_name": "ns_vpnvserver"}	console_ns_vpnvserver

见解	JSON	要使用的表名
Gateway Insight (3)	{ "adc_ip_address": "10.106.186.141", "gateway_name": "vpn_vserver_141_7", "rpt_sample_time": 1702011308, "sessions": 1, "table_name": "af_vpn_session_details", "users": 1 }	console_af_vpn_session_details
Gateway Insight (4)	{ "active_sessions": 59, "active_users": 1, "adc_ip_address": "10.106.186.136", "gateway_name": "vpnathul2", "rpt_sample_time": 1698919848, "table_name": "af_vpn_active_session_1"}	console_af_vpn_active_session_1
Gateway Insight (5)	{ "adc_ip_address": "10.106.186.136", "entity_type": 3, "gateway_name": "vpnathul2", "hits": 3, "rpt_sample_time": 1698052438, "table_name": "af_vpn_error_reports" }	console_af_vpn_error_reports

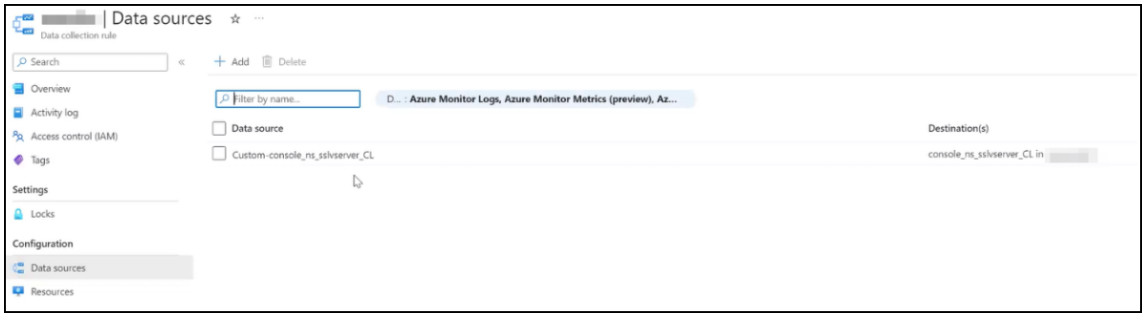
上载 JSON 后，您可以查看以下详细信息：

单击“转换编辑器”，输入以下适用于相应见解的查询，然后单击“运行”，在 NetScaler 控制台中接受从轮询开

始的数据。

- **SSL** - `source | extend TimeGenerated = todatetime(poll_time)| project-rename sslvserver_id = id`
- **WAF** 和机器人-`source | extend TimeGenerated = todatetime(rpt_sample_time)`
- **Gateway Insight** - `source | extend TimeGenerated = todatetime(rpt_sample_time)`

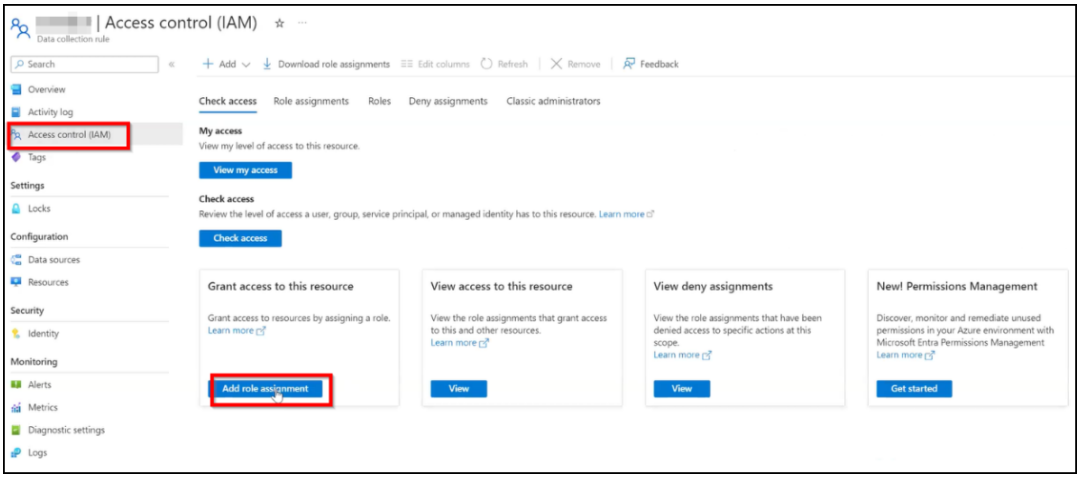
5. 单击“下一步”，然后单击“创建”以完成。
6. 导航到 数据收集规则，单击您创建的 DCR。
7. 在“配置”下，单击“数据源”以查看创建的表。



DCR（数据收集规则）需要访问监视指标发布者角色。

a) 在“最近”下导航到可以从 Azure 门户访问的 DCR。

b) 在您的 DCR 页面上单击访问控制 **(IAM)**，然后单击添加角色分配。



c) 在搜索栏中，键入关键字 monitor 以选择“监视指标发布者”，然后单击“下一步”。

d) 在“成员”选项卡中，单击“选择成员”，然后选择您创建的 Entra 应用程序。

e) 单击 **Review + assign**（检查 + 分配）。

您必须记下数据收集规则 ID。导航到数据收集规则页面，选择您的 DCR，然后单击 JSON 视图以记下 ID。

在 **NetScaler** 控制台中创建订阅

您现在一切都准备好了。最后一步是通过创建订阅并添加所需的详细信息来配置 NetScaler 控制台。要在 NetScaler 控制台中创建订阅，您需要记下以下细节：

- 端点 URL
- 数据收集规则 ID
- 租户 ID
- 客户端 ID
- 客户端密钥

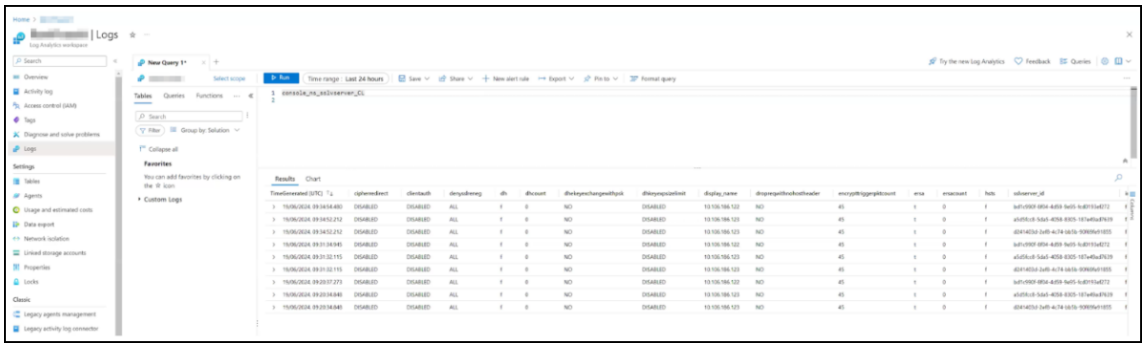
1. 登录到 NetScaler 控制台。

2. 导航到“设置”**>**“可观测性集成”。
3. 在“集成”页面中，单击“添加”。
4. 在“创建订阅”页面中，指定以下详细信息：
    a) 在“订阅名称”字段中指定您选择的名称。
    b) 选择 **NetScaler** 控制台作为源，然后单击“下一步”。
    c) 选择 **Microsoft Sentinel**，然后单击“配置”。在“配置终端节点”页面中，输入所有详细信息，然后单击“提交”。
    d) 单击下一步。
5. 单击“添加见解”，在“选择功能”选项卡中，根据您在 Microsoft Azure 中添加的表，选择要导出的功能，然后单击“添加选定功能”，然后单击“下一步”。
6. 在“选择实例”选项卡中，可以选择“选择所有实例”或“自定义选择”，然后单击“下一步”。
    - 选择所有实例 - 将所有 NetScaler 实例中的数据导出到 Microsoft Sentinel。
    - 自定义选择 - 允许您从列表中选择 NetScaler 实例。如果您从列表中选择特定实例，则数据将仅从选定的 NetScaler 实例导出到 Microsoft Sentinel。
7. 单击 **Submit**（提交）。

在 **Microsoft Azure** 中查看日志

配置完所有内容后，我们建议您等到 30 分钟才能在 Microsoft Azure 中查看细节。

1. 在您的 Azure 门户中，导航到您的日志分析工作区。
2. 单击“日志”，提供表名，然后单击“运行”以查看结果。



配置 **NetScaler** 实例，使用默认架构将见解导出到 **Prometheus**

September 2, 2024

NetScaler 支持直接将指标导出到 Prometheus。您可以使用 NetScaler 实例提供的丰富指标来监视 NetScaler 运行状况和应用程序运行状况。例如，您可以收集有关 CPU 和内存使用情况的指标以了解 NetScaler 的运行状况。同样，您可以使用每秒收到的 HTTP 请求数或活跃客户端数量等指标来监视应用程序运行状况。

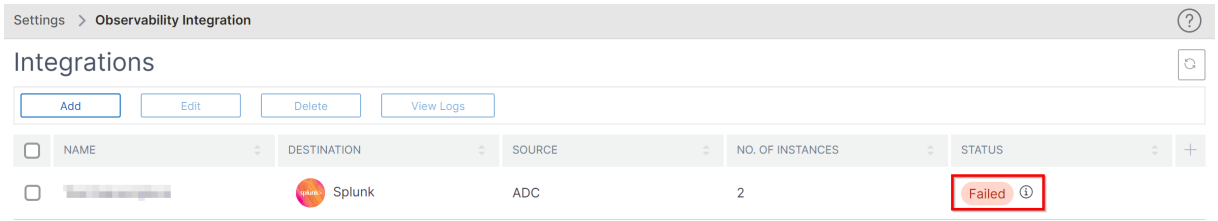
要将指标导出到 Prometheus，必须配置类型为时间序列的分析配置文件。有关更多信息，请参阅使用 Pro metheus 监视 NetScaler、应用和应用安全。

使用 NetScaler 控制台中的可观测性集成功能，您可以使用默认架构配置将见解导出到 Prometheus。

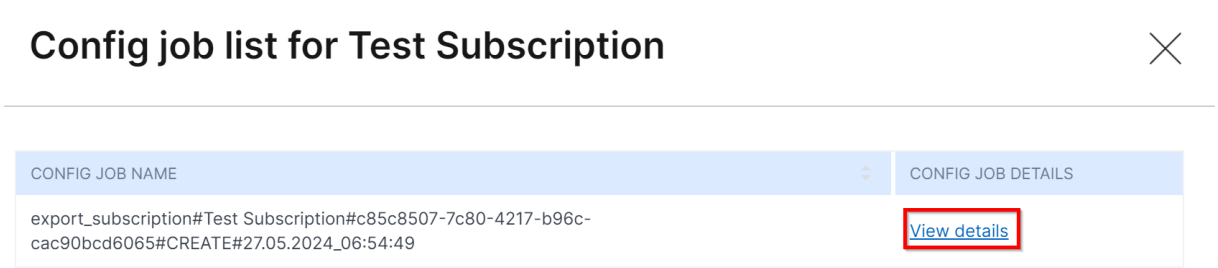
1. 导航到“设置”**>**“可观测性集成”。
2. 在“集成”页面中，单击“添加”。
3. 在“创建订阅”页面中，指定以下详细信息：
    a) 在“订阅名称”字段中指定您选择的名称。
    b) 选择 **NetScaler** 作为来源，然后单击“下一 步”。
    c) 选择 **Prometheus** 作为目标。
    d) 选择“默认”以获得导出的默认见解。
    e) 单击“添加实例”，然后选择要将见解导出到 Prometheus 的实例。
    f) 单击 **Submit**（提交）。

查看失败配置的日志

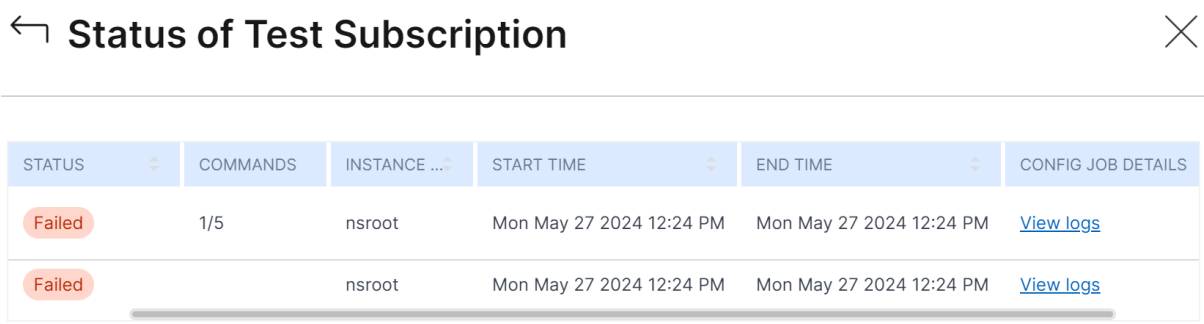
创建订阅后，可以在设置 **>** 可观测性集成中查看已创建订阅的状态。如果状态显示失败，请单击查看详细信息。



单击配置作业详细信息下的查看详细信息。



单击查看日志以查看问题的详细信息。



配置将 **NetScaler** 指标和审核日志导出到 **Splunk**

September 2, 2024

NetScaler 支持将指标以 JSON 格式直接导出到 Splunk。NetScaler 提供了丰富的指标来监视您的应用程序运行状况和应用程序安全运行状况。通过将 NetScaler 提供的指标导出到 Splunk，您可以对指标进行可视化并获得有意义的见解。

审核日志记录使您能够记录 NetScaler 状态和由 NetScaler 中各种模块收集的状态信息。通过查看日志，您可以解决问题或错误并进行修复。

有关详细信息，请参阅：

- 将审核日志直接从 NetScaler 导出到 Splunk
- 将指标直接从 NetScaler 导出到 Splunk

要配置通过 NetScaler 控制台将指标和审核日志导出到 Splunk，请执行以下操作：

1. 导航到“设置”**>**“可观测性集成”。
2. 在“集成”页面中，单击“添加”。
3. 在“创建订阅”页面中，指定以下详细信息：
    a) 在“订阅名称”字段中指定您选择的名称。
    b) 选择 **NetScaler** 作为来源，然后单击“下一 步”。
    c) 选择 **Splunk** 作为目标，然后单击“配置”。在“配置端点”中：
        - 端点 **URL** - 指定 Splunk 端点的详细信息。终点必须采用以下 <`https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event`>‘ 格式。
        - 身份验证令牌 - 从 Splunk 复制并粘贴身份验证令牌。
        - 单击 **Submit**（提交）。

d) 单击下一步。

e) 单击“添加见解”，选择“**NetScaler** 指标和 **NetScaler** 审核日志”，然后单击“添加选定内容”。

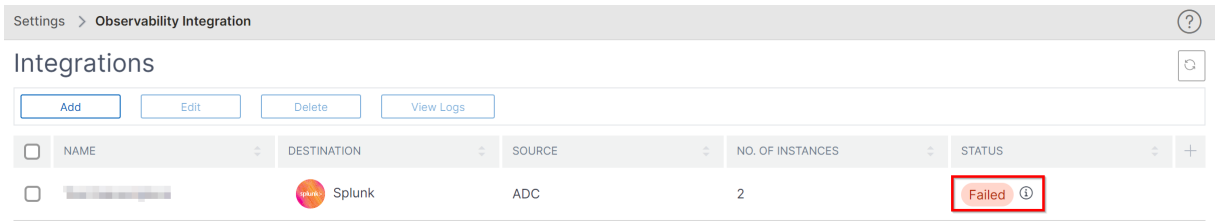
f) 单击下一步。

g) 单击“添加实例”，然后选择实例。

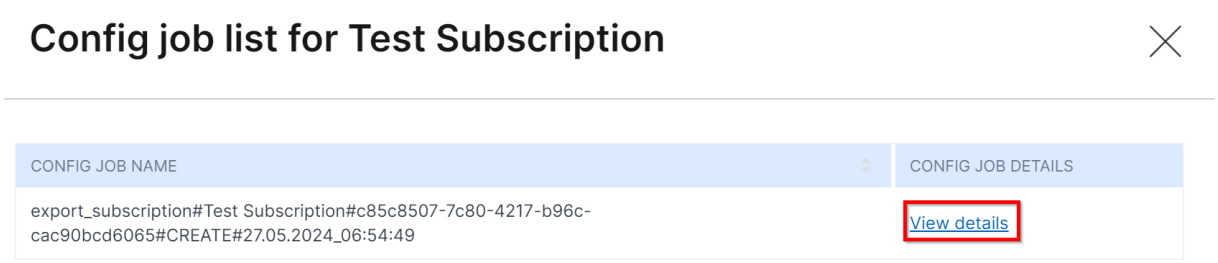
h) 单击 **Submit**（提交）。

查看失败配置的日志

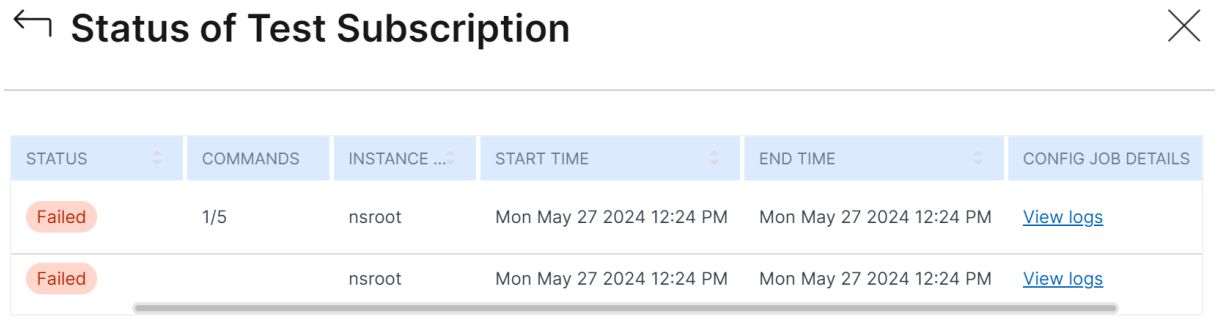
创建订阅后，可以在设置 **>** 可观测性集成中查看已创建订阅的状态。如果状态显示失败，请单击查看详细信息。



单击配置作业详细信息下的查看详细信息。



单击查看日志以查看问题的详细信息。



配置分析设置

January 29, 2024

在开始使用 NetScaler 控制台上的分析功能来查看您的实例和应用数据之前，建议您配置一些分析设置，以确保使用此功能获得最佳体验。

为分析创建阈值和警报

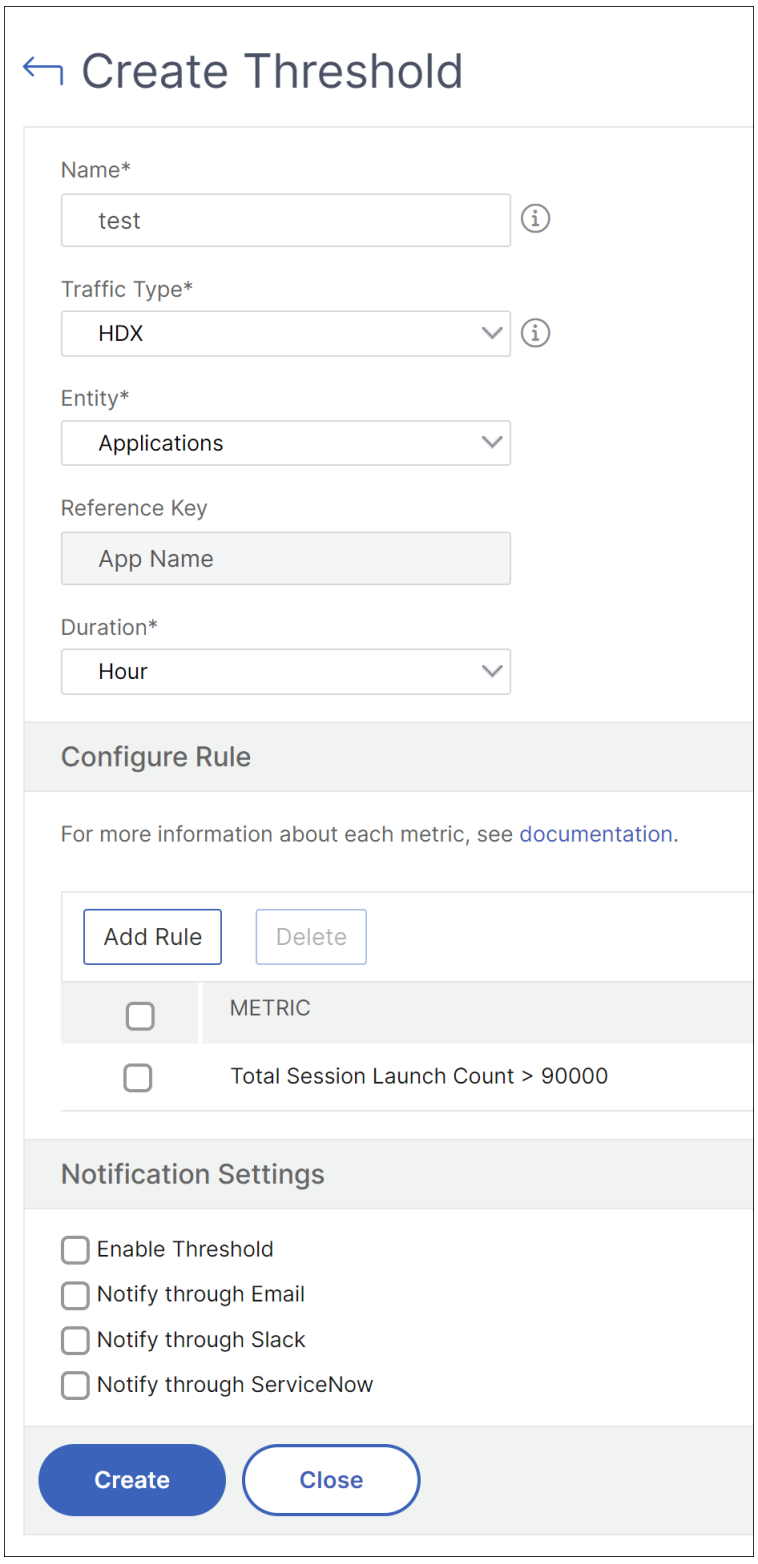
您可以设置阈值和警报，以监视在发现的实例上配置的托管虚拟服务器的分析指标。当指标的值超过阈值时，NetScaler 控制台会生成一个表示违反阈值的事件。

您还可以将操作与设置的阈值相关联。操作包括在 GUI 上显示警报、按配置发送电子邮件。

例如，您可以设置阈值，以便在任何用户的 ICA RTT 值超过 1 秒时为 HDX Insight 生成事件。您还可以为生成的事件启用警报，并将阈值违反信息发送到配置的电子邮件列表。

要创建用于分析的阈值和警报：

1. 导航到设置 > 分析设置 > 阈值。
2. 在“阈值”屏幕上，单击“添 加”以添加新阈值并为设置的阈值配置警报。
3. 在 **Create Thresholds and Alerts**（创建阈值和警报）页面上，指定以下详细信息：
    - **Name**（名称）- 用于配置阈值的名称。
    - 流量类型 -要为其配置阈值的分析流量的类型。例如：HDX Insight、Security Insight。
    - **Entity**（实体）- 要为其配置阈值的类别或资源类型。
    - **Reference Key**（引用键）- 根据选择的流量类型和实体自动生成的值。
    - **Duration**（持续时间）- 要为其配置阈值的时间间隔。
4. 要配置电子邮件通知，请选中设置阈值的复选框。
5. 在“规则”部分中，指定以下内容：
    - 指标 -所选流量类型的指标，用于配置阈值。
    - 比较器—所选指标的比较器（例如：<、> =）。
    - 值 -用于设置阈值和调用警报的指标的值。
6. 单击创建。



配置通知

January 29, 2024

您可以选择通知类型来接收以下功能的通知：

- 事件—为 NetScaler 实例生成的事件列表。有关详细信息，请参阅 添加事件规则操作。
- 许可证—当前处于活动状态、即将到期等的许可证列表。有关更多信息，请参见 NetScaler 控制台许可到期。
- **SSL** 证书—添加到 NetScaler 实例的 SSL 证书列表。有关详细信息，请参阅 SSL 证书过期

NetScaler 控制台支持以下通知类型：

- 电子邮件
- SMS
- Slack
- PagerDuty
- ServiceNow

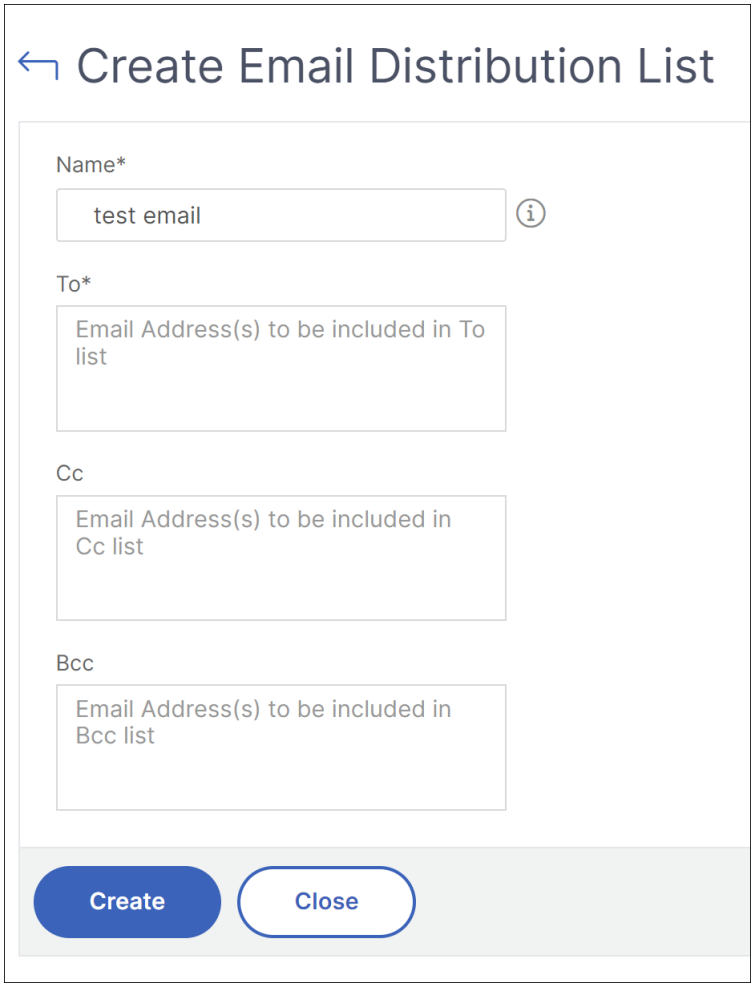
对于每种通知类型，NetScaler 控制台 GUI 会显示已配置的分发列表或配置文件。NetScaler 控制台向选定的分发列表或配置文件发送通知。

创建电子邮件通讯组列表

要接收有关 NetScaler 控制台功能的电子邮件通知，必须添加邮件服务器和分发列表。

执行以下步骤创建电子邮件通讯组列表：

1. 导航到“设置”**>**“通知”。
2. 在 电子邮件中，单击 添加。
3. 在 创建电子邮件通讯组列表中，指定以下详细信息：
    - 名称 -指定通讯组列表名称。
    - 收件人-指 定 NetScaler 控制台必须向其发送消息的电子邮件地址。
    - 抄送-指定 NetScaler 控制台必须向其发送消息副本的电子邮件地址。
    - 密件 **@@** 抄送-指定 NetScaler 控制台在不显示地址的情况下必须向其发送消息副本的电子邮件地址。



4. 单击创建。

重复此过程以创建多个电子邮件通讯组列表。“邮件”标签显示 NetScaler 控制台中存在的所有邮件分发列表。

创建 **SMS** 分发列表

要接收有关 NetScaler 控制台功能的短信通知，必须添加 SMS 服务器和电话号码。

执行以下步骤配置 SMS 通知设置：

1. 导航到“设置”**>**“通知”。
2. 在 **SMS** 中，单击 添加。
3. 在“创建 **SMS** 分发列表”中，指定以下详细信息：
   - 名称 -指定通讯组列表名称。
   - **SMS** 服务器 -选择发送 SMS 通知的 SMS 服务器。
   - 收件人-指 定 NetScaler 控制台必须向其发送消息的电话号码。

4. 单击创建。

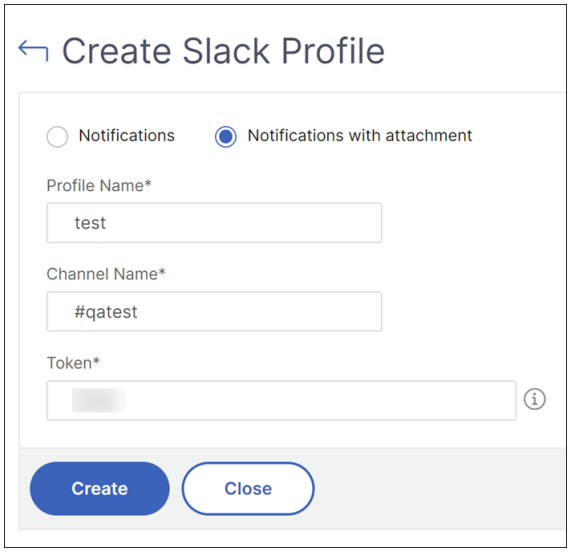
重复此步骤创建多个 SMS 通讯组列表。**SMS** 标签显示了 NetScaler 控制台中存在的所有 SMS 分发列表。

创建 **Slack** 配置文件

要接收有关 NetScaler 控制台功能的 Slack 通知，必须创建 Slack 配置文件。

执行以下步骤来创建“Slack”配置文件：

1. 导航到“设置”**>**“通知”。
2. 在“**Slack**”中，单击“添加”。
3. 在 创建 **Slack** 配置文件中，指定以下详细信息：
   - 配置文件名称 -指定配置文件名称。此名称显示在 Slack 配置文件列表中。
   - 频道名称 -指定 NetScaler 控制台必须向其发送通知的 Slack 频道名称。
   - **Webhook URL** -指定该频道的 Webhook URL。传入的 Webhook 是将来自外部来源的消息发布到 Slack 的简单方法。URL 在内部链接到频道名称。而且，所有事件通知都会发送到此 URL 上的指定 Slack 频道。webhook 的一个例子如下：https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. 单击创建。

重复此过程创建多个 Slack 配置文件。**Slack** 标签显示了 NetScaler 控制台中存在的所有 Slack 配置文件。

创建 **PagerDuty** 配置文件

您可以添加 PagerDuty 配置文件来监视基于 PagerDuty 配置的事件通知。使用 PagerDuty，您可以通过电子邮件、短信、推送通知和电话在注册号码上配置通知。

在 NetScaler 控制台中添加 PagerDuty 配置文件之前，请确保您已在 PagerDuty 中完成所需的配置。要开始使用 PagerDuty，请参阅 PagerDuty 文档。

请执行以下步骤来创建 PagerDuty 配置文件：

1. 导航到“设置”**>**“通知”。
2. 在“**PagerDuty**”中，单击“添加”。
3. 在 创建 **PagerDuty** 配置文件中，指定以下详细信息：
    - 配置文件名称 -指定您选择的配置文件名称。
    - 集成密钥 -指定集成密钥。您可以从您的 PagerDuty 门户网站获取此密钥。
4. 单击创建。

有关更多信息，请参阅 PagerDuty 文档中的 服务和集成 。

重复此过程以创建多个 PagerDuty 配置文件。**PagerDuty** 标签显示了 NetScaler 控制台中存在的所有 PagerDuty 配置文件。

查看 **ServiceNow** 配置文件

当您想为 NetScaler 事件和 NetScaler 控制台事件启用 ServiceNow 通知时，必须使用 ITSM 连接器将 NetScaler 控制台与 ServiceNow 集成在一起。有关更多信息，请参见 将 NetScaler 控制台与 ServiceNow 实例集成。

执行以下步骤以查看和验证 ServiceNow 配置文件：

1. 导航到“设置”**>**“通知”。
2. 在“**ServiceNow**”中，从列表中选择 **Citrix_Workspace_SN** 配置文件。
3. 单击“测试”自动生成 ServiceNow 票证并验证配置。

    如果您想在 NetScaler 控制台 GUI 中查看 ServiceNow 票证，请选择 **ServiceNow** 票证。

导出或计划导出报告

January 29, 2024

在 NetScaler 控制台中，您可以导出所选 NetScaler 控制台功能的综合报告。此报告为您概述了实例、分区之间的映射以及相应的详细信息。

NetScaler 控制台在各个 NetScaler 控制台功能下显示特定功能的计划导出报告，您可以查看、编辑或删除这些报告。例如，要查看 NetScaler 实例的导出报告，请导航到 基础结构 **>** 实例 **> NetScaler** ，然后单击导出图标。您可以以 PDF、JPEG、PNG 和 CSV 文件格式导出这些报告。

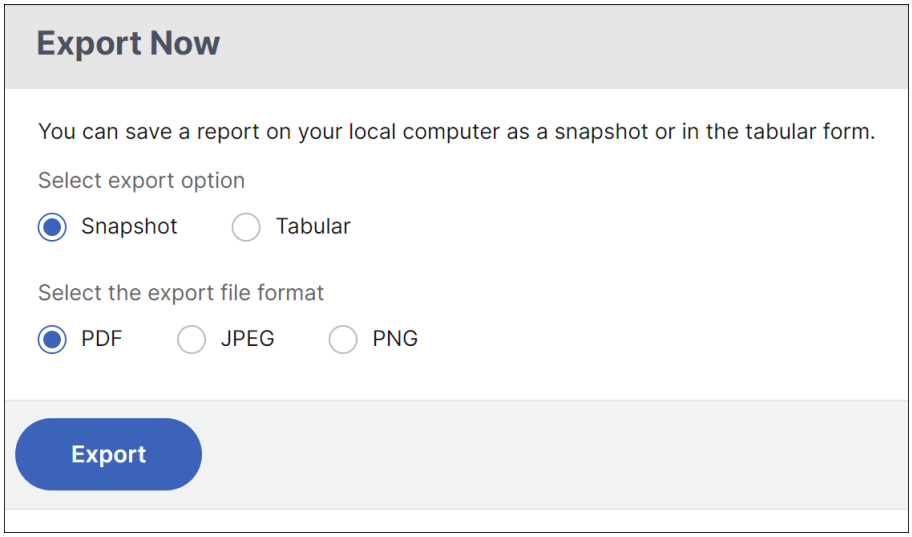
在“导出报告”中，您可以执行以下操作：

- 将报告导出到本地计算机
- 安排导出报告
- 查看、编辑或删除预定的导出报告

导出报告

要将报告从 NetScaler 控制台导出到本地计算机，请执行以下步骤：

1. 单击页面右上角的导出图标。
2. 选择“立即导出”。
3. 选择以下导出选项之一：
    - 快照-此选项将 NetScaler 控制台报告导出为快照。
    - 表格-此选项以表格格式 导出 NetScaler 控制台报告。您还可以选择以表格格式导出的数据记录数



4. 选择要在本地计算机上保存报告的文件格式。
5. 单击导出。

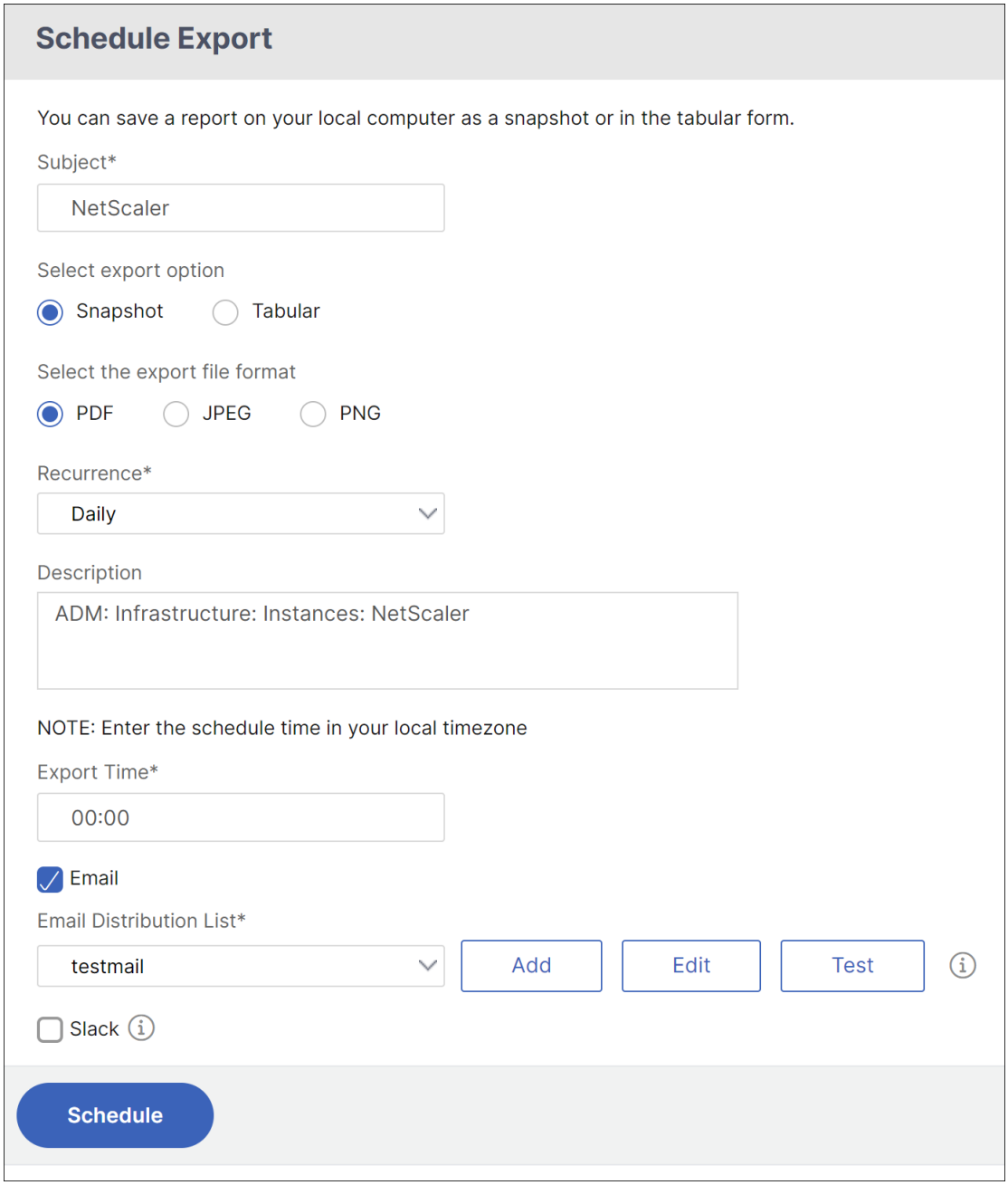
安排导出报告

要定期安排导出报告，请指定重复间隔。NetScaler 控制台将导出的报告发送到配置的电子邮件或 slack 配置文件。

1. 单击页面右上角的导出图标。
2. 选择 计划导出 并指定以下内容：
    - 主题 -默认情况下，此字段会自动填充选定的功能名称。但是，您可以使用有意义的标题重写它。

- 导出选项 -以快照或表格格式导出 NetScaler 控制台报告。您还可以选择以表格格式导出的数据记录数
- 格式 -选择要在配置的电子邮件或松弛配置文件上接收报告的文件格式。
- 循环 -从列表中选择“每日”、“每周”或“每 月”。
- 说明 -为报表指定有意义的描述。
- 导出时间 -指定要导出报告的时间。
- 电子邮件 - 选中复选框并从列表框中选择配置文件。如果要添加配置文件，请单击“添加”。
- **Slack** - 选中复选框并从列表框中选择配置文件。如果要添加配置文件，请单击“添加”。

3. 单击 **Schedule**（计划）。



查看和编辑计划的导出报告

要查看导出报告，请执行以下操作：

1. 单击页面右上角的导出图标。

   导出报告 页面显示所有特定功能的导出报告。

2. 选择要编辑的报告，然后单击 编辑。

实例设置

January 29, 2024

您可以在 NetScaler 控制台中管理发现的实例并配置实例备份设置。

管理实例配置

在 设置 **>** 全局设置 **>** 实例设置 **>** 实例管理中，您可以修改以下实例配置：

- 与实例通信 **-**您可以在 NetScaler 控制台和发现的实例之间选择 HTTP 或 HTTPS 通信信道。
- 启用证书下载 -允许您从已发现的实例下载 SSL 证书。
- 提示实例登录凭据 -当您通过 NetScaler 控制台 GUI 访问实例时，将显示实例登录页面。指定您的登录凭据以访问实例。

配置实例备份设置

在 设置 **>** 全局设置 **>** 实例设置 **>** 实例备份中，您可以在 NetScaler 控制台中为发现的 NetScaler 实例配置备份设置。

在 配置实例备份设置中，选择 启用实例备份。

- 要保留的备份文件数量：指定要在 NetScaler 控制台中保留的备份文件数量。每个 NetScaler 实例最多可以保留 3 个备份文件。默认为 1 个备份文件。
- 备份计划设置-您可以通过两种方式计划实例备份：
  - 基于间隔 **-**在指定的间隔过后，在 NetScaler 控制台中创建备份文件。默认备份时间间隔是 12 小时。
  - 基于时间-以 您希望 `hours:minutes`NetScaler 控制台进行实例备份的 格式指定时间。
- **NetScaler** 设置-使用此选项，您可以根据陷阱启动备份，并在备份中包含 GeoDB 文件。此设置适用于 MPX、VPX、CPX 和 BLX 实例。
  - 收到 **NetScalerConfigSave** 陷阱时进行实例备份**-**默认情况下，NetScaler 控制台在收到 “NetScaler-ConfigSave” 陷阱时不会创建备份文件。但是，每当 NetScaler 实例向 NetScaler 控制台发送 陷阱时，您都可以启用创建备份文件的`NetScalerConfigSave`选项。

    每次保存实例上的配置时，NetScaler 实例都会发送 `NetScalerConfigSave`。

    指定 陷阱延迟时备份（以分钟为单位）。如果收到的 陷`NetScalerConfigSave`阱在 NetScaler 控制台上持续了指定的分钟数，则 NetScaler 控制台会备份该实例。

  - 包含 **GeoDB** 文件 -默认情况下，NetScaler 控制台不备份地理数据库文件。您也可以启用该选项以创建这些文件的备份。

- **NetScaler SDX** 设置 -要备份 SDX 实例，请指定备份超时（以分钟为单位）。在 SDX 实例备份期间，NetScaler 控制台和 SDX 之间的连接将在指定的时间段内保持不变。

  对于大型 SDX 备份文件，请在 NetScaler 控制台和 SDX 实例之间保持更长时间的连接，以确保备份完成。

  > 重要：
  >
  > 如果连接超时，备份将失败。

- 外部传输 -NetScaler 控制台允许您将 NetScaler 实例备份文件传输到外部位置：

  1. 指定位置的 IP 地址。
  2. 指定要将备份文件传输到的外部服务器的用户名和密码。
  3. 指定传输协议和端口号。
  4. 指定必须存储文件的目录路径。
  5. 如果要在将文件传输到外部服务器后删除备份文件，请选择在 传输后从 **Application Delivery Management** 中删除文件。

实例设置

January 29, 2024

您可以在 NetScaler 控制台中管理发现的实例并配置实例备份设置。

管理实例配置

在 设置 **>** 全局设置 **>** 实例设置 **>** 实例管理中，您可以修改以下实例配置：

- 与实例通信 **-**您可以在 NetScaler 控制台和发现的实例之间选择 HTTP 或 HTTPS 通信信道。
- 启用证书下载 -允许您从已发现的实例下载 SSL 证书。
- 提示实例登录凭据 -当您通过 NetScaler 控制台 GUI 访问实例时，将显示实例登录页面。指定您的登录凭据以访问实例。

配置实例备份设置

在 设置 **>** 全局设置 **>** 实例设置 **>** 实例备份中，您可以在 NetScaler 控制台中为发现的 NetScaler 实例配置备份设置。

在 配置实例备份设置中，选择 启用实例备份。

- 要保留的备份文件数量：指定要在 NetScaler 控制台中保留的备份文件数量。每个 NetScaler 实例最多可以保留 3 个备份文件。默认为 1 个备份文件。
- 备份计划设置-您可以通过两种方式计划实例备份：
  - 基于间隔 **-**在指定的间隔过后，在 NetScaler 控制台中创建备份文件。默认备份时间间隔是 12 小时。
  - 基于时间-以 您希望 `hours:minutes`NetScaler 控制台进行实例备份的 格式指定时间。
- **NetScaler** 设置-使用此选项，您可以根据陷阱启动备份，并在备份中包含 GeoDB 文件。此设置适用于 MPX、VPX、CPX 和 BLX 实例。
  - 收到 **NetScalerConfigSave** 陷阱时进行实例备份**-**默认情况下，NetScaler 控制台在收到 “NetScaler-ConfigSave” 陷阱时不会创建备份文件。但是，每当 NetScaler 实例向 NetScaler 控制台发送 陷阱时，您都可以启用创建备份文件的`NetScalerConfigSave`选项。

    每次保存实例上的配置时，NetScaler 实例都会发送 `NetScalerConfigSave`。

    指定 陷阱延迟时备份（以分钟为单位）。如果收到的 陷`NetScalerConfigSave`阱在 NetScaler 控制台上持续了指定的分钟数，则 NetScaler 控制台会备份该实例。
  - 包含 **GeoDB** 文件 -默认情况下，NetScaler 控制台不备份地理数据库文件。您也可以启用该选项以创建这些文件的备份。
- **NetScaler SDX** 设置 -要备份 SDX 实例，请指定备份超时（以分钟为单位）。在 SDX 实例备份期间，NetScaler 控制台和 SDX 之间的连接将在指定的时间段内保持不变。

  对于大型 SDX 备份文件，请在 NetScaler 控制台和 SDX 实例之间保持更长时间的连接，以确保备份完成。

  > 重要：
  >
  > 如果连接超时，备份将失败。

- 外部传输 -NetScaler 控制台允许您将 NetScaler 实例备份文件传输到外部位置：
  1. 指定位置的 IP 地址。
  2. 指定要将备份文件传输到的外部服务器的用户名和密码。
  3. 指定传输协议和端口号。
  4. 指定必须存储文件的目录路径。
  5. 如果要在将文件传输到外部服务器后删除备份文件，请选择在 传输后从 **Application Delivery Management** 中删除文件。

系统配置

January 29, 2024

您可以修改 NetScaler 控制台代理的保持活动间隔和 NetScaler 控制台服务器时区。

设置座席的保持活动时间间隔

NetScaler 控制台服务器和代理在指定的保持连接间隔内保持相同的 TCP 连接。代理使用此连接将托管实例数据发送到 NetScaler 控制台服务器。

1. 导航到 设置 **>** 全局设置。
2. 选择“系统配置”下的“代理和时区”。
3. 在 **Agent** 中，指定在 30-120 秒之间的保持活动时间间隔。
4. 单击保存。

设置 **NetScaler** 控制台的时区

您可以选择要在 NetScaler 控制台网页、通知和报告中显示时间的时区。

1. 导航到 设置 **>** 全局设置。
2. 选择“系统配置”下的“代理和时区”。
3. 在 时区中，选择本地或 GMT 时区以在 NetScaler 控制台中显示时间。
4. 单击保存。

电子邮件订阅

January 29, 2024

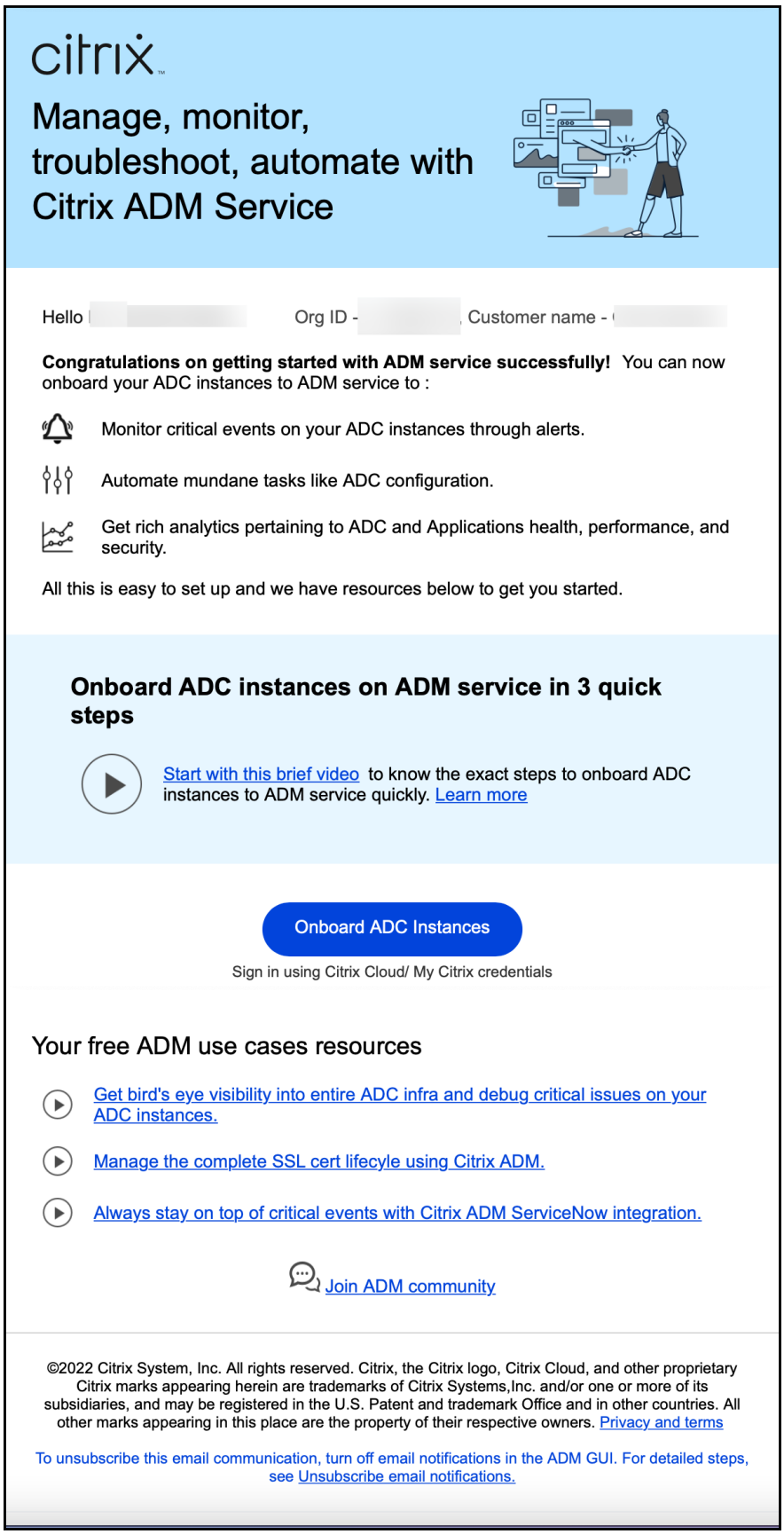
NetScaler 控制台向所有非活动用户和新用户发送电子邮件通知。

在以下情况下，不活跃的客户会收到电子邮件通知：

- 未配置 NetScaler 实例
- 租户许可证将在 30 天内过期

> 注意：
>
> 默认情况下，所有此类不活跃的客户都会收到一封电子邮件通知。

新客户会收到一封来自 NetScaler 控制台的电子邮件，邀请他们将 NetScaler 实例加入 NetScaler 控制台服务，在那里他们能够管理和监视 NetScaler 实例上的关键事件、进行故障排除和自动执行诸如 NetScaler 配置之类的任务。



citrix

Manage, monitor, troubleshoot, automate with Citrix ADM Service

Hello Org ID - Customer name -

Congratulations on getting started with ADM service successfully! You can now onboard your ADC instances to ADM service to :

- Monitor critical events on your ADC instances through alerts.
- Automate mundane tasks like ADC configuration.
- Get rich analytics pertaining to ADC and Applications health, performance, and security.

All this is easy to set up and we have resources below to get you started.

Onboard ADC instances on ADM service in 3 quick steps

Start with this brief video to know the exact steps to onboard ADC instances to ADM service quickly. Learn more

Onboard ADC Instances

Sign in using Citrix Cloud/ My Citrix credentials

Your free ADM use cases resources

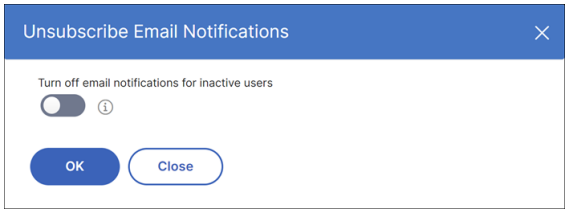
- Get bird's eye visibility into entire ADC infra and debug critical issues on your ADC instances.
- Manage the complete SSL cert lifecyle using Citrix ADM.
- Always stay on top of critical events with Citrix ADM ServiceNow integration.

Join ADM community

取消订阅电子邮件通知

您可以订阅或取消订阅从 NetScaler 控制台服务收到的电子邮件通知。要 取消订阅电子邮件通知，请执行以下操作：

1. 在 NetScaler 控制台中，导航 到“设置”**>**“全局 设置”**>**“系统配置”，然后单击“电子邮件订阅”。将出现“取消订阅电子邮件通知”窗口。



> 注意：
>
> 默认情况下，用于关闭电子邮件通知的切换按钮处于关闭位置，所有不活跃用户的电子邮件通知处于启用状态。

2. 在“取消订阅电子邮件通知”窗口中，打开切换按钮。单击确定。

您现在已取消订阅邮件通知，不会收到任何发往 Onboard NetScaler 实例的邮件。

启用或禁用功能

July 17, 2024

作为管理员，您可以在“设置”>“全局设置”**>**“可配置功能”页面中启用或禁用以下功能：

- 代理故障切换 -代理故障切换可能发生在具有两个或多个活动代理的站点上。当站点中的代理处于非活动状态（关闭状态）时，NetScaler 控制台会将该非活动代理的 NetScaler 实例与其他活动代理一起重新分发。有关详细信息，请参阅为多站点 部署配置 NetScaler 代理代理。
- 实体轮询网络功能 -实体可以是附加到 NetScaler 实例的策略、虚拟服务器、服务或操作。默认情况下，NetScaler 控制台每 60 分钟自动轮询配置的网络功能实体。有关详细信息，请参阅 轮询概述。
- 实例备份-备份 NetScaler 实例的当前状态，然后使用备份的文件将 NetScaler 实例恢复到相同状态。有关更多信息，请参阅 备份和还原 NetScaler 实例。
- 实例配置审核 -跨托管 NetScaler 实例监视配置更改，排除配置错误并恢复未保存的配置。有关详细信息，请参阅 创建审核模板。
- 实例事件 -事件表示在托管 NetScaler 实例上发生的事件或错误。在 NetScaler 控制台中收到的事件显示在“事件摘要”页面（“基础架构”**>**“事件”）上。所有活动事件都显示在“事件消息”页面（基础结构 **>** 事件 **>** 事件消息）中。有关更多信息，请参阅 事件。

- 实例网络报 告-您可以在全局级别为实例生成报告。此外，适用于虚拟服务器和网络接口等实体。有关详细信息，请参阅 网络报告。
- 实例 **SSL** 证书 -NetScaler 控制台提供安装在所有托管 NetScaler 实例上的 SSL 证书的集中视图。有关详细信息，请参阅 SSL 控制面板。
- 实例 **Syslog**-如果您已将设备配置为将所有系统日志消息重定向到 NetScaler 控制台，则可以监视在 NetScaler 实例上生成的系统日志事件。有关更多信息，请参阅在 实例上配置 syslog。

要启用功能，请执行以下步骤：

1. 从列表中选择要启用的功能。
2. Click **Enable**。

> 重要：
>
> 如果禁用某项功能，则用户无法执行与该功能相关的操作。

配置操作策略以接收应用程序事件通知

March 10, 2024

除了现有的应用程序事件分析视图外，您还可以配置操作策略以通过 Slack、Email、PagerDuty 或 ServiceNow 获取应用程序事件通知。应用程序事件包括性能问题、机器人和 WAF 违规以及服务图违规。作为管理员，使用操作策略，您可以实时获取事件通知。

使用操作策略，您可以：

- 为应用程序事件预定义某些条件。
- 通过 Slack、Email、PagerDuty 和 ServiceNow 获取有关以下事件的通知：

活动类别	活动子类别	事件
安全违规	所有安全违规行为	所有机器人违规行为（有关机器人违规清单的更多信息，请参阅 违规类别）。 所有 WAF 违规（WAF SQL 违规、WAF XSS 违规和 WAF 推断 XML 违规）
	每个客户端的所有安全违规事件	每个客户端的机器人违规行为 每个客户端的 WAF 违规情况

活动类别	活动子类别	事件
		注意：要收到 WAF 违规通知，最低违规交易量必须为 20%。例如，在 100 笔交易中，至少有 20 笔必须是违规交易。
应用程序性能		应用程序得分违规
		客户端网络延迟
		服务器网络延迟
		服务器处理时间
		响应时间
		请求
		Bandwidth（带宽）
		服务图表违规
应用程序使用情况		每秒的请求
		吞吐量
		Data Volume（数据量）

配置操作策略

1. 导航到 设置 **>** 操作 **>** 操作策略。
2. 单击添加。
3. 在“创建操作策略”页面中：
   a) 策略名称—提供您选择的策略名称。
   b) 启用 -默认情况下，此选项处于选中状态。
   c) 如果 发生以下事件 -从列表中选择一个事件。
   d) 并且“满足以下条件”—从列表中选择定义要收到通知的条件。您可以单击 **+** 添加更多条件。要删除条件，请单击 —。

      您可以使用以下运算符配置操作策略。根据您选择的条件显示运算符。

操作员	说明
等于	等于一个定义的值
不等于	不等于定义的值
大于	大于定义的值
大于或等于	大于或等于定义的值
小于	小于定义的值
小于或等于	小于或等于定义的值
包含	包含已定义的术语或值
开头是	以已定义的术语或值开头
结尾为	以定义的术语或值结尾
IN	允许您选择多个值

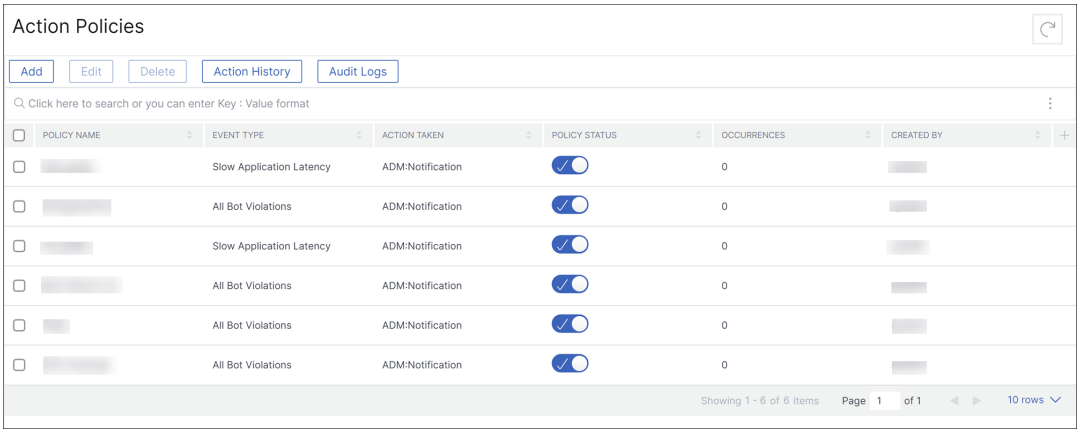
e) 然后执行以下操作—选择“通知”。选择“通知”后，将显示“通知类型”选项。

f) 通知类型—选择通知类型电子邮件、Slack、PagerDuty 或 ServiceNow。根据您选择的通知类型，会出现相应的选项（分发列表、Slack 配置文件、PagerDuty 配置文件或 ServiceNow 配置文件）。从列表中选择配置文件。

如果要创建新的配置文件，请单击“添加”。

g) 单击创建策略。

策略已配置。您可以查看配置的策略详细信息。



配置策略后，可以选择策略并单击：

- 编辑 以更新或更改操作策略。更新后，单击“更新策略”。
- 删除 可移除操作策略。您可以选择多个策略，然后单击“删除”将其删除。

- 操作历史记录 可查看时间、采取的操作、策略名称、警报类型和警报消息等详细信息。

下表描述了操作策略配置的详细信息。

违规名称	条件	说明
所有安全违规行为	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	违规次数	您希望收到通知的违规次数。例如，如果您将违规计数配置为小于或等于 10，则当收到的机器人违规交易少于 10 笔时，您将收到通知。
	违规率	该值表示来自特定交易的违规总数，该值必须介于 0 和 1 之间。例如，在 100 笔交易中，有 20 笔是违规行为，如果您想收到此类情况的通知，则必须输入 0.2。
所有机器人违规行为	机器人档案	机器人配置文件名称，用于在 NetScaler 实例上配置机器人管理。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	违规次数	您希望收到通知的违规次数。例如，如果您将违规计数配置为小于或等于 10，则当收到的机器人违规交易少于 10 笔时，您将收到通知。
	违规率	该值表示来自特定交易的违规总数，该值必须介于 0 和 1 之间。例如，在 100 笔交易中，有 20 笔是违规行为，如果您想收到此类情况的通知，则必须输入 0.2。
所有 **WAF** 违规、**WAF SQL** 违规、**WAF XSS** 违规、**WAF** 推断 **XML** 违规	WAF 配置文件	用于在 NetScaler 实例上配置 WAF 安全设置的 WAF 配置文件名称。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	违规次数	您希望收到通知的违规次数。WAF 违规行为收到通知的最低要求为 20%。

违规名称	条件	说明
	违规率	该值表示来自特定交易的违规总数，该值必须介于 0 和 1 之间。例如，在 100 个事务中，20 个是 WAF SQL 违规事务，如果您想收到此类情况的通知，则必须输入 0.2。
每个客户端的所有安全违规事件	应用程序名称	自定义应用程序名称。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	客户端 IP	机器人起源的来源。指定 IP 地址。
	Total Attacks（攻击总数）	您希望收到通知的攻击总数。
	请求 URL	您要配置为屏蔽的 URL。指定 URL。
	虚拟服务器名称	为自定义应用程序配置的关联应用程序。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
每个客户端的机器人违规行为	应用程序名称	自定义应用程序名称。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	客户端 IP	机器人起源的来源。指定 IP 地址。
	Total Attacks（攻击总数）	您希望收到通知的攻击总数。
	违规类型	从列表中选择机器人违规。
	请求 URL	您要配置为屏蔽的 URL。指定 URL。
	虚拟服务器名称	为自定义应用程序配置的关联应用程序。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
每个客户端的 **WAF** 违规情况	应用程序名称	自定义应用程序名称。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。

违规名称	条件	说明
	实例 IP	NetScaler 实例的 IP 地址。从列表中选择 IP 地址。
	客户端 IP	机器人起源的来源。指定 IP 地址。
	Total Attacks（攻击总数）	您希望收到通知的攻击总数。
	违规类型	从列表中选择 WAF 违规行为。
	请求 URL	您要配置为屏蔽的 URL。指定 URL。
	虚拟服务器名称	为自定义应用程序配置的关联应用程序。从列表中选择应用程序。如果您不添加此条件，则会考虑 NetScaler 实例中的所有应用程序。
应用程序得分违规	绩效指标	应用程序评分组成部分及其阈值。从列表中选择应用程序评分组件。有关更多信息，请参阅 选择 App Score 组件和设置阈值。
	漏洞计数	您想要收到通知的漏洞数量。例如，如果您将响应时间的漏洞计数配置为 5，则当超过响应时间阈值 5 次时，您将收到通知。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。
客户端网络延迟	客户端网络平均延迟	指定要收到通知的客户端延迟（客户端到 NetScaler）值（以毫秒为单位）。
	客户端网络延迟异常	指定您希望收到 通知的网络延迟的异常次数。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。
服务器网络延迟	服务器网络平均延迟	指定要收到通知的服务器延迟（服务器到 NetScaler）值（以毫秒为单位）。
	服务器网络延迟异常	指定您希望收到 通知的网络延迟的异常次数。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。
响应时间	平均响应时间	指定要接收通知的值（以毫秒为单位）。
	响应平均时间异常	指定要收到通知的异常次数。

违规名称	条件	说明
	应用程序名称	单击“选择应用程序”以选择要接收通知的应用程序。如果您未选择任何应用程序，则该应用程序将应用于所有应用程序。
请求	请求总数	指定要收到通知的请求总数。
	应用程序名称	单击“选择应用程序”以选择要接收通知的应用程序。如果您未选择任何应用程序，则该应用程序将应用于所有应用程序。
Bandwidth（带宽）	总带宽	指定要接收通知的带宽 (MB)。
	应用程序名称	单击“选择应用程序”以选择要接收通知的应用程序。如果您未选择任何应用程序，则该应用程序将应用于所有应用程序。
服务器处理时间	服务器处理平均时间	指定要收到通知的服务器处理（服务器到 NetScaler）值（以毫秒为单位）。
	服务器处理时间异常	指定您希望收到通知的服务器处理时间的异常次数。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。
服务图违规		违反配置阈值的微服务。有关更多信息，请参阅在服务图表中配置阈值。
每秒的请求	平均每秒请求数	应用程序每秒收到的请求数。指定要获得通知的平均值。
	每秒平均请求数异常	指定您想要获得通知的平均异常次数。 注意：如果您对此事件使用 AND 条件，则可以配置每秒平均请求数和应用程序名称或每秒请求异常平均值和应用程序名称。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。
吞吐量	平均吞吐量	特定时间段内传输的总数据。指定要获得通知的平均值（以 MB 为单位）。
	吞吐量平均异常	指定您想要获得通知的平均异常次数。

违规名称	条件	说明
		注意：如果您对此事件使用 AND 条件，则可以配置吞吐量平均值和应用程序名称或吞吐量平均异常和应用程序名称。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。
Data Volume（数据量）	总数据量	在特定时长内要传输的总数据。指定要接收通知的值（以 MB 为单位）。
	数据量异常	指定要收到通知的异常次数。
		注意：如果您对此事件使用 AND 条件，则可以配置“总数据量和应用程序名称”或“数据量异常和应用程序名称”。
	应用程序名称	单击“选择应用程序”，选择要通知违规行为的应用程序。

使用搜索栏

搜索栏允许您筛选结果。当您点击搜索栏时，它会给您一个搜索建议列表。您可以选择组件并根据要求筛选结果。

使用审核日志选项

单击“审核日志”，从列表中选择持续时间以查看在所选持续时间内创建、修改和删除的操作策略，然后单击“搜索”。

> 注意
>
> 预计在即将发布的版本中，数据存储政策将发生变化。通过这些更改，历史数据在超过存储限制后将无法存储。目前，建议添加更多存储空间或将存储空间保持在许可证授权限制范围内。

使用审核日志来管理和监视您的基础结构

March 10, 2024

您可以使用 NetScaler 控制台来跟踪 NetScaler 控制台上的所有事件以及在 NetScaler 实例上生成的系统日志事件。这些消息可以帮助您管理和监视基础结构。但是，只有当您查看日志消息时，它们才是很好的信息来源，NetScaler 控制台简化了查看日志消息的方式。

您可以使用过滤器搜索 NetScaler 控制台的系统日志和审核日志消息。过滤器有助于缩小结果范围，并实时准确找到您要查找的内容。内置的“Search Help”（搜索帮助）将指导您筛选日志。查看日志消息的另一种方法是将其导出为 PDF、CSV、PNG 和 JPEG 格式。您可以计划以各种时间间隔将这些报告导出到指定的电子邮件地址。

您可以从 NetScaler 控制台 GUI 中查看以下类型的日志消息：

- NetScaler 实例相关的审核日志
- 与 NetScaler 控制台相关的审核日志
- 应用程序审核日志

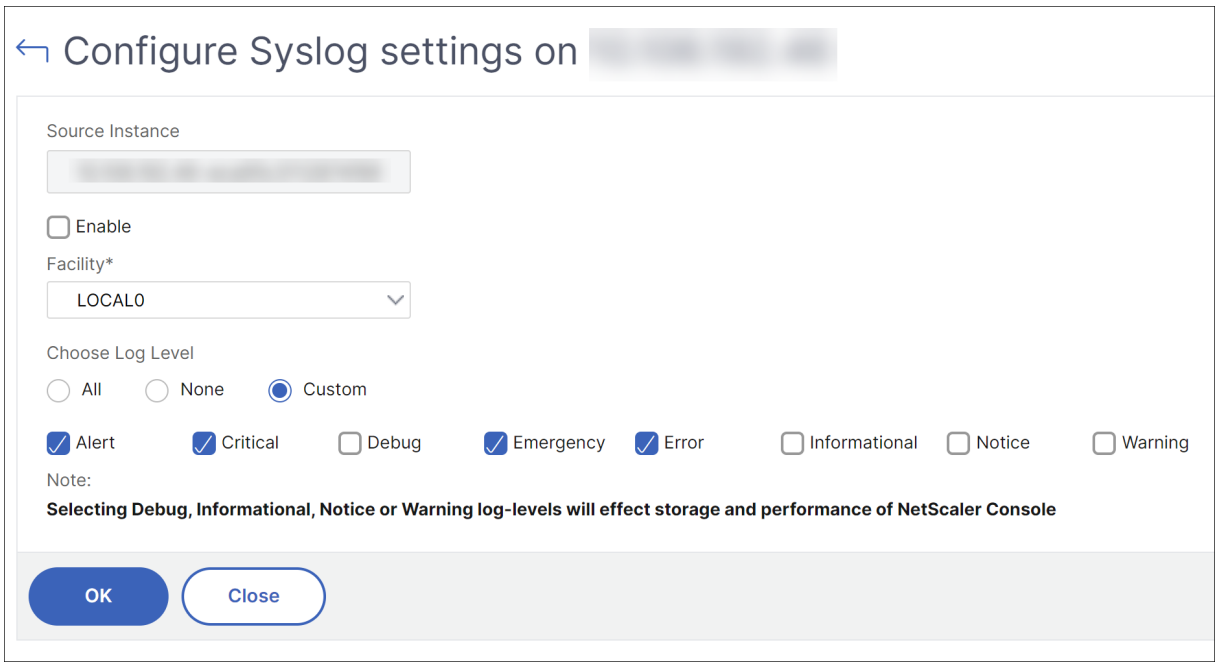
NetScaler 实例相关的审核日志

在从 NetScaler 控制台查看与 NetScaler 实例相关的系统日志消息之前，请将 NetScaler 控制台配置为 NetScaler 实例的系统日志服务器。配置完成后，所有系统日志消息都将从实例重定向到 NetScaler 控制台。

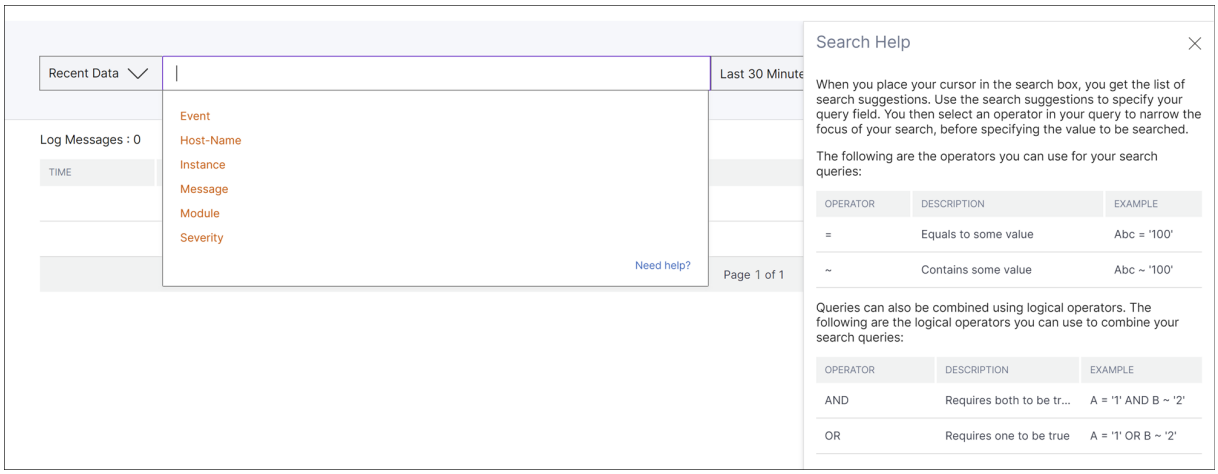
将 NetScaler 控制台配置为系统日志服务器

按照以下步骤将 NetScaler 控制台配置为系统日志服务器：

1. 在 NetScaler 控制台 GUI 中，导航 到基础架构 **>** 实例。
2. 选择要从中收集系统日志消息并在 NetScaler 控制台中显示的 NetScaler 实例。
3. 在 **Select Action**（选择操作）列表中，选择 **Configure Syslog**（配置 Syslog）。
4. Click **Enable**。
5. 在 **Facility**（设施）下拉列表中，选择本地或用户级别的设施。
6. 为 syslog 消息选择所需的日志级别。
7. 单击确定。



这些步骤配置 NetScaler 实例中的所有系统日志命令，然后 NetScaler 控制台开始接收系统日志消息。您可以通过导航到 **Infrastructure**（基础结构）**> Events**（事件）**> Syslog Messages**（**syslog** 消息）来查看消息。单击 **Need Help?**（需要帮助?）打开内置的搜索帮助。有关更多信息，请参阅 查看和导出 syslog 消息。



要导出日志消息，请单击右上角的箭头图标。

下一步，单击 **Export Now**（立即导出）或 **Schedule Export**（计划导出）。有关更多信息，请参阅 导出 syslog 消息。

与 **NetScaler** 控制台相关的审核日志

根据预先配置的规则，NetScaler 控制台为所有事件生成审核日志消息，帮助您监视基础架构的运行状况。要查看 NetScaler 控制台中存在的所有审核日志消息，请导航 到“设置”**->**“审核日志消息”。

要导出日志消息，请单击右上角的箭头图标。

与应用程序相关的审核日志

您可以查看所有 NetScaler 控制台应用或特定应用的审核日志消息。

- 要查看 NetScaler 控制台中存在的所有应用程序的所有审核日志消息，请导航 到基础架构 **>** 网络功能 审核。
- 要在 NetScaler 控制台中查看任何特定应用程序的审核日志消息，请导航 到应用程序 **>** 控制面板 **>** 双击虚拟服务器 审核日志。

> 注意
>
> 您可以将 NetScaler 控制台审核日志消息转发到外部服务器。有关详细信息，请参阅 查看审核信息。

配置 **IP** 地址管理 **(IPAM)**

January 29, 2024

NetScaler 控制台 IPAM 允许您在 NetScaler 控制台托管配置中自动分配和释放 IP 地址。您可以从使用以下 IP 提供程序定义的网络或 IP 范围分配 IP：

- NetScaler 控制台内置 IPAM 提供程序。
- 信息布鲁 IPAM 解决方案。

可以在以下环境中使用 NetScaler 控制台 IPAM：

- 样书：创建配置时自动将 IP 分配给虚拟服务器。
- **API** 网关：自动向 API 代理分配 IP 地址。

您还可以跟踪每个网络中的 IP 地址或由 NetScaler 控制台管理的 IP 范围。

添加外部 **IP** 地址提供商

NetScaler 控制台内置了 IPAM 提供程序，用于管理 IP 和 IP 范围。您也可以使用 NetScaler 控制台的外部 IP 地址提供程序。

> 重要：
>
> 在开始之前，请确保已在外部 IP 地址提供程序中启用以下权限：
>
> - 能够查询提供商中存在的网络。
> - 在网络中预留 IP 地址。
> - 从网络中释放 IP 地址。

> - 从网络中检索使用的 IP 地址。
> - 从网络中检索可用的 IP 地址。

执行以下步骤，在 NetScaler 控制台中添加外部 IPAM 提供商解决方案：

1. 导航到 设置 **> IPAM**。
2. 在 提供程序中，单击 添加。
3. 指定以下详细信息以添加 IPAM 提供程序：
   - 名称 - 指定要在 NetScaler 控制台中使用的 IP 提供商名称。
   - 供应商 -从列表中选择 IPAM 供应商。
   - **URL**-指定在 NetScaler 控制台环境中分配 IP 地址的 IPAM 解决方案的 URL。确保使用以下格式指定 URL：

     ```
     1  https://<host name>
     ```

     示例：`https://myinfoblox.example.com`
   - 用户名 -指定要登录 IPAM 解决方案的用户名。
   - 密码 -指定用于登录 IPAM 解决方案的密码。
4. 单击添加。

Infoblox DDI 作为外部提供商

目前，NetScaler 控制台支持 Infoblox DDI 作为外部提供商。

您可以将 NetScaler 控制台 IPAM 与 Infoblox 提供商一起使用来执行以下操作：

- 列出 IPAM 网络
- 创建、更新和删除 IPAM 网络
- 从 IPAM 网络中保留和释放 IP 地址

创建 **IPAM** 网络　要使用 Infoblox 提供商创建 NetScaler 控制台 IPAM 网络，Infoblox 上必须存在具有相同 CIDR IP 范围的网络。

当您在 NetScaler 控制台中创建 IPAM 网络时，您只能在 NetScaler 控制台中注册 Infoblox 网络的使用。然后，NetScaler 控制台与 Infoblox 协同工作，管理从网络分配的 IP 地址。InfoBlox 网络可以继续在 NetScaler 控制台之外使用。

同样，如果您删除 NetScaler 控制台 IPAM 网络，NetScaler 控制台会注销 Infoblox 网络。这意味着，NetScaler 控制台不再与 Infoblox 交互以进行该网络中的 IP 地址管理。

Infoblox DDI API NetScaler 控制台 IPAM 使用以下 Infoblox API 来执行相应的操作：

- (/network) - 列出所有可用的 Infoblox 网络
- (/network?network={id}) - 检索特定 Infoblox 网络的详细信息
- (/ipv4address) - 列出 Infoblox 网络上的所有 IP
- (/record:host) - 检索特定 IP 地址的详细信息
- (/{IP}) - 在 Infoblox 网络上保留和释放 IP

> 注意：
>
> - Infoblox DNS、DHCP 和 IP 地址管理 (DDI) 服务器 IP 和端口必须可以从公共网络访问，这样 NetScaler 控制台服务才能访问并连接到 Infoblox 服务器。
> - 在 NetScaler 控制台上配置的 Infoblox 用户帐户必须具有使用 Infoblox API 所需的权限。

有关 Infoblox API 的更多信息，请参阅 Infoblox DDI 上提供的 Infoblox REST API 参考指南。

添加网络

添加一个网络以使用 IPAM 和 NetScaler 控制台托管配置。

1. 导航到 设置 **> IPAM**。
2. 在“网络”下，单击“添加”。
3. 指定以下详细信息：
    - 网络名称 -在 NetScaler 控制台中指定用于标识网络的网络名称。
    - 提供商 -从列表中选择提供商。

      此列表显示在 NetScaler 控制台中添加的提供商。
    - 网络类型 -根据您的要求从列表中选择 **IP** 范围 或 **CIDR** 。
    - 网络值 -指定网络值。

      > 注意：
      >
      > NetScaler 控制台 IPAM 仅支持 IPv4 地址。

      对于 **IP** 范围，请按以下格式指定网络值：

      ```
      <first-IP-address>-<last-IP-address>
      ```

      示例：

      ```
      10.0.0.20-10.0.0.100
      ```

      对于 **CIDR**，请按以下格式指定网络值：


```
<IP-address>/<subnet-mask>
```

示例：

```
10.70.124.0/24
```

4. 单击创建。

查看分配的 **IP** 地址

要查看有关从 IPAM 网络分配的 IP 地址的更多详细信息，请执行以下步骤：

1. 导航到 设置 **> IPAM**。
2. 在“网络”选项卡下，单击“查看所有分配的 **IP**”。

   此窗格显示 IP 地址、提供商名称、提供商供应商和描述。它还显示保留此 IP 地址的资源详细信息：

   - 模块：显示保留 IP 地址的 NetScaler 控制台模块。例如，如果样书保留了 IP 地址，则此列将样书显示为模块。
   - 资源类型：显示该模块中的资源类型。对于样书模块，只有配置资源类型使用 IPAM 网络。因此，它会在此列下显示配置。
   - 资源 **ID**：显示带链接的确切资源 ID。单击此链接可访问使用 IP 地址的资源。对于配置资源类型，它将配置包 ID 显示为资源 ID。

> 注意：
>
> 如果要释放 IP 地址，请选择要释放的 IP 地址，然后单击“释放分配的 **IP**”。

操作方法文章

August 8, 2024

NetScaler 控制台的“操作文章”是有关该服务可用功能的简单、相关且易于实现的文章。这些文章包含有关一些常用 NetScaler 控制台功能的信息，例如实例管理、配置管理、事件管理、应用程序管理、样书和证书管理。

单击下表中的功能名称可查看该功能的操作方法文章列表。

主题		
实例管理	配置管理	证书管理

样书	主题
	事件管理

实例管理

如何监视分布全球的站点

如何管理 NetScaler 实例的管理分区

如何向 NetScaler 控制台添加实例

如何在 NetScaler 控制台上创建实例组

如何在 NetScaler 控制台中轮询 NetScaler 实例和实体

如何在 NetScaler 控制台中为地理地图配置站点

如何强制故障转移到辅助 NetScaler 实例

如何强制辅助 NetScaler 实例保持辅助状态

如何更改 NetScaler MPX 或 VPX 根密码

如何更改 NetScaler SDX 根密码

配置管理

如何在配置作业中使用 SCP (put) 命令

如何使用 NetScaler 控制台升级 NetScaler SDX 实例

如何在 NetScaler 控制台中安排使用内置模板创建的作业

如何重新安排在 NetScaler 控制台中使用内置模板配置的作业

重用运行配置作业

如何使用 NetScaler 控制台升级 NetScaler 实例

如何在 NetScaler 控制台上创建配置作业

如何在 NetScaler 控制台的配置任务中使用变量

如何使用配置模板在 NetScaler 控制台上创建审核模板

如何在 NetScaler 控制台上使用更正命令创建配置作业

如何在 NetScaler 控制台上将正在运行和保存的配置命令从一个 NetScaler 实例复制到另一个 NetScaler 实例

如何使用配置作业将配置从一个实例复制到多个实例

如何在 NetScaler 控制台上使用主配置模板

证书管理

如何在 NetScaler 控制台上配置企业策略

如何从 NetScaler 控制台在 NetScaler 实例上安装 SSL 证书

如何从 NetScaler 控制台更新已安装的证书

如何使用 NetScaler 控制台关联和取消链接 SSL 证书

如何使用 NetScaler 控制台创建证书签名请求 (CSR)

如何设置来自 NetScaler 控制台的 SSL 证书到期通知

如何在 NetScaler 控制台上使用 SSL 控制面板

样书

如何在 NetScaler 控制台中使用默认样书

如何创建自己的样书

如何在 NetScaler 控制台中使用用户定义的样书

如何使用 API 基于样书创建配置

如何对在样书中定义的虚拟服务器启用分析和配置警报

如何创建样书以将 SSL 证书和证书密钥文件上载到 NetScaler Console

如何在企业中使用 Microsoft Skype for Business 样书

如何在企业中使用 Microsoft Exchange 样书

如何在企业中使用 Microsoft SharePoint 样书

如何使用 Microsoft ADFS Proxy 样书

如何使用 Oracle 电子商务样书

如何使用 SSO Office 365 样书

如何使用 SSO Google Apps 样书

事件管理

如何在 NetScaler 控制台上为事件设置事件时长

如何使用 NetScaler 控制台安排事件过滤器

如何为来自 NetScaler 控制台的事件设置重复的电子邮件通知

如何使用 NetScaler 控制台抑制事件

如何使用事件控制板来监视事件

如何在 NetScaler 控制台上创建事件规则

如何修改 NetScaler 实例上发生的事件的报告严重性

如何在 NetScaler 控制台中查看事件摘要

如何在 NetScaler 控制台上显示 SNMP 陷阱的事件严重性和 SNMP 陷阱偏差

如何使用 NetScaler 控制台导出系统日志消息

如何在 NetScaler 控制台中抑制 Syslog 消息

常见问题解答

June 7, 2024

我需要安装多少代理

代理的数量取决于数据中心中托管实例的数量和总吞吐量。Citrix 建议您为每个数据中心至少安装一个代理。

如何安装多个代理

首次登录该服务时，只能安装一个代理。要添加多个代理，首先完成初始设置，然后导航到 设置 > 安装代理。

NetScaler 代理支持 **AMD** 处理器吗

是。

我可以从内置代理过渡到外部代理吗

是的，您可以。有关更多信息，请参阅从内置代理过渡到外部代理。

如果我丢失了新的激活码，如何获得新的激活码

如果您是首次加入，请访问服务 GUI，导航到“设置代理”屏幕，然后单击“生成激活码”。

尝试安装第二个代理时，要生成新的激活码，请导航到 基础结构 **>** 实例 **>** 代理 **>** 生成激活码。

如何登录代理虚拟机？什么是默认凭据

如果您的代理安装在虚拟机管理程序或 Microsoft Azure 云上，则该代理的默认登录凭据是 `nsrecover/nsroot`，这将打开代理的 shell 提示符。

如果您的代理安装在 AWS 上，则登录代理的默认凭据为 `nsrecover/instance id`。

在本地虚拟机管理程序上安装代理程序的资源需求是什么

32 GB 内存、8 个虚拟 CPU、500 GB 存储空间、1 个虚拟网络接口、1 Gbps 吞吐量

在置备时，我是否需要为代理分配额外的磁盘

不，您不必添加额外的磁盘。该代理仅用作 NetScaler 控制台与企业数据中心或云端实例之间的中介。它不存储需要额外磁盘的库存或分析数据。

我可以使用多个代理重复使用激活码吗

不，您不能。

如果我输入的值不正确，如何重新运行网络设置

访问虚拟机管理程序上的代理控制台，使用凭据 ns 恢复/nsroot 登录到 shell 提示符，然后运行命令 `networkconfig`。

如果我的代理注册失败，我该怎么办

请确保：

- 您的代理可以访问互联网（配置 DNS）。
- 您已正确复制激活码。
- 您输入的服务 URL 正确。
- 您已打开所需的端口。

注册成功，但如何知道代理是否正常运行呢

成功注册代理后，访问 NetScaler 控制台并导航到“设置 代理”屏幕。您可以在屏幕上看到发现的代理。如果代理运行良好，则会出现绿色图标。如果它没有运行，则会出现一个红色图标。

如何使用代理服务器将代理连接到 **NetScaler** 控制台

您可以使用代理服务器将代理连接到 NetScaler 控制台。该脚本可在代理中的 `/mps` 文件夹中找到。代理将其所有数据转发到代理服务器，然后代理服务器通过互联网将数据发送到 NetScaler 控制台。

要使用代理服务器转发数据，请使用以下脚本在代理上键入代理服务器的详细信息：`proxy_input.py`，然后按照脚本提供的说明输入更多信息。代理在使用代理服务器连接到 NetScaler 控制台时会获取此信息。

您可以通过提供用户名和密码信息对代理服务器进行身份验证。当代理发送数据时，代理服务器会对用户凭据进行身份验证，然后再将其转发到 NetScaler 控制台。

有关更多信息，请参见 作为 API 代理服务器的 NetScaler 控制台。

> 注
>
> 意 NetScaler 控制台支持启用基本身份验证的代理服务器。NetScaler 控制台还支持禁用身份验证的代理服务器。

我没有看到我的分析报告

在虚拟服务器上启用洞察以查看分析报告。有关详细信息，请参阅 启用分析。

NetScaler 控制台支持哪些版本的 **NetScaler** 实例

对于管理和监视功能，支持运行 10.5 及更高版本的 NetScaler 实例。某些功能仅在某些 NetScaler 版本上受支持。有关详细信息，请参阅系统要求。

如何在 **NetScaler** 控制台中导出控制面板报告

要在 NetScaler 控制台中导出任何控制面板的报告，请单击此页面右上角的“导出”图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
   报告将下载到您的系统。
2. 选择 计划报告 以设置定期生成和导出报告的计划。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

   a) 循环 -从下拉列表框中选择 每日、每周 或每 月。

   > 注意
   >
   > - 如果您选择每周定期，请确保您选择要计划报表的工作日。
   > - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

b) 循环时间 -以 24 小时格式输入时间 Hour： Minute。

c) 电子邮件 -选中该复选框，然后从下拉列表框中选择配置文件，或单击 添加 以创建电子邮件配置文件。

d) **Slack** - 选中复选框，然后从下拉列表框中选择配置文件，或单击“添加”以创建电子邮件配置文件。

单击 启用计划 以计划您的报告，然后单击 确定。通过单击 启用计划 复选框，您可以生成选定的报告。

启用客户端测量有什么作用

启用客户端测量后，NetScaler 控制台通过 HTML 注入捕获 HTML 页面的加载时间和呈现时间指标。使用这些指标，管理员可以识别 L7 延迟问题。

从代理到 **NetScaler** 控制台服务的 **SSL** 流量是否通过 **SSL** 检查获取

我们建议您绕过代理的 SSL 检查，转到 NetScaler 控制台服务 SSL 流量。